

Handbuch Datenschutz

Datum	03. May 2018
Autor	MKM / FLO
Revisor	CPF
Version	2.2

Inhaltsverzeichnis

1	Einführung	2
2	Definitionen	3
3	Gesetzliche Anforderungen	3
4	Funktionen und Merkmale von SecuTix 360°	5
4.1	Rechtmäßigkeit des Zwecks und der Verarbeitung der Daten	5
4.2	Verarbeitung nach Treu und Glauben und Transparenz der Datenerhebung und - verarbeitung	6
4.3	Angemessenheit, Zweckdienlichkeit und strenge Notwendigkeit der Daten.....	7
4.4	Nutzung von Cookies auf der Web-Schnittstelle oder im Web-Modul	13
4.5	Speicherdauer der Daten	17
4.6	Korrekte, aktualisierte Daten. Recht auf Zugang, Berichtigung, Löschung und Übertragbarkeit. Recht auf Einschränkung der Verarbeitung und Widerspruchsrecht gegen Verarbeitung.....	18
4.7	Datensicherheit	21
4.8	Auftragsverarbeiter, Unterauftragsverarbeiter und grenzüberschreitende Datenströme.....	23
4.9	Nutzung von Daten zu Marketingzwecken.....	24
4.10	Formalitäten	27
	Anhang 1. Von Ihrer Einrichtung auszufüllende Checkliste zur Verarbeitung personenbezogener Daten in der Lösung SecuTix 360°	29
	Anhang 2. Liste der Unterauftragsverarbeiter von SecuTix SA	31

1 Einführung

Als Einrichtung, die die Lösung SecuTix 360° nutzt, erheben und verarbeiten Sie als für die Verarbeitung zuständige Person personenbezogene Daten insbesondere Ihrer Kunden, die Tickets kaufen, Ihrer potenziellen Kunden, Ihrer Mitarbeiter, etc. Diese Daten können auch von SecuTix SA in seiner Eigenschaft als Auftragsverarbeiter zum Zwecke der Lieferung dieser Lösung sowie der Leistungen oder Services, deren Erbringung Sie mit uns abgeschlossen haben, weitergegeben und/oder verarbeitet werden.

Im Rahmen der Erhebung, Verarbeitung und Weitergabe dieser personenbezogenen Daten müssen Sie die geltende Gesetzgebung zum Schutz personenbezogener Daten einhalten. Für die Einhaltung dieser für Sie im Bereich des Datenschutzes geltenden Anforderungen sind Sie als für die Verarbeitung zuständige Person verantwortlich.

In der Europäischen Union (EU) beruht die geltende Gesetzgebung auf der Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (der sog. DSGVO), die in allen EU-Mitgliedstaaten ab dem 25. Mai 2018 anwendbar ist.

SecuTix SA unterliegt der Schweizer Gesetzgebung zum Datenschutz (siehe nachstehender Rahmen). Diese Rechtsvorschrift ist der der EU-Länder sehr ähnlich, in einigen Punkten sogar mit ihr identisch. Per Entscheidung der Europäischen Kommission 2000/518/EG vom 26.07.2000 wurde die Schweiz als Land anerkannt, das einen angemessenen Schutz der personenbezogenen Daten aus Ländern der EU gewährleistet.

Daher stellt Ihnen SecuTix SA eine Lösung zur Verfügung, die es Ihnen ermöglicht, die diesbezüglichen europäischen Bestimmungen einzuhalten. Nachstehend erläutern wir Ihnen (ohne Anspruch auf Vollständigkeit) die technischen und organisatorischen Möglichkeiten, die SecuTix 360° diesbezüglich bietet.

Vorbemerkung

Vorab wird darauf hingewiesen, dass:

- dieses Datenschutzhandbuch einzig und allein zum Ziel hat, Ihnen die in der Lösung SecuTix 360° enthaltenen Funktionen im Hinblick auf Sensibilisierung und Information vorzustellen, da es sich um von uns getroffene Vorsichtsmaßnahmen handelt, damit Sie bestimmte gesetzliche Bestimmungen einhalten können, die für Sie als für die Datenverarbeitung verantwortliche Person zutreffen könnten;
- dieses Dokument keinesfalls als Anweisung oder Ratschlag mit rechtlicher Bedeutung zu verstehen ist;
- die Festlegung der Zwecke und Mittel der Datenverarbeitung einzig und allein Ihre Entscheidung ist, für die nur Sie verantwortlich sind; Sie müssen uns daher Ihre Maßnahmen anhand der Checkliste in Anhang 1 mitteilen.

2 Definitionen

Personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Syn. in diesem Dokument „Personendaten“);

Verarbeitung: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Verkettung solcher Vorgänge im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden (Syn. in diesem Dokument „Sie“, „Ihre Einrichtung“);

Auftragsverarbeiter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Syn. in diesem Dokument „wir“, „SecuTix SA“);

Betroffene Person: natürliche Person, deren personenbezogene Daten im Rahmen der Nutzung der Lösung SecuTix 360° verarbeitet werden;

Verletzung des Schutzes personenbezogener Daten: eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

3 Gesetzliche Anforderungen

Gemäß den europäischen Rechtsvorschriften muss jeder Verantwortliche folgende Grundsätze einhalten:

- die Erhebung und die Verarbeitung der Daten müssen den folgenden Grundsätzen entsprechen: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
- der Zweck der Datenverarbeitung muss festgelegt, eindeutig und legitim sein. Die personenbezogenen Daten dürfen später nicht zu Zwecken verarbeitet werden, die als mit den ursprünglichen Zwecken unvereinbar gelten;

- die erhobenen und verarbeiteten Daten müssen dem Zweck angemessen und zweckdienlich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Sie müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Sensible Daten dürfen nur unter bestimmten Bestimmungen erhoben und verarbeitet werden, insbesondere mit Einwilligung der betroffenen Personen;
- die Speicherdauer der Daten darf nicht überhöht sein, sondern muss im Hinblick auf den oder die Zwecke der Datenverarbeitung verhältnismäßig sein;
- die betroffenen Personen müssen über die Verarbeitung ihrer personenbezogenen Daten informiert werden; für bestimmte Verarbeitungen ist ihre Einwilligung einzuholen. Die den betroffenen Personen mitzuteilenden Informationen müssen eine Reihe verbindlicher Hinweise enthalten;
- den betroffenen Personen muss ein Recht auf Zugang, Berichtigung, Löschung und Übertragbarkeit ihrer Daten gewährt werden sowie ein Recht auf Beschränkung der Datenverarbeitung und ein Widerspruchsrecht auf die Verarbeitung der besagten Daten. Die betroffenen Personen verfügen darüber hinaus über das Recht, nicht Gegenstand einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zu sein, einschließlich der Profilierung, die rechtliche Auswirkungen auf diese Personen hat oder sie in ähnlicher Weise erheblich beeinträchtigt;
- geeignete technische und organisatorische Maßnahmen sind zu treffen, damit die Sicherheit der Daten, insbesondere der Schutz vor Zugang oder Vernichtung, Veränderung oder nicht autorisierter Veröffentlichung der besagten Daten, gewährleistet ist (in bestimmten Fällen ist eine Auswirkungsanalyse erforderlich, um die geeigneten Maßnahmen zu bewerten; daraus kann sich die Verpflichtung ergeben, die zuständige Aufsichtsbehörde zu konsultieren). Verletzungen des Schutzes personenbezogener Daten unterliegen einem speziellen Meldungsprozess bei der zuständigen Aufsichtsbehörde, unter bestimmten Umständen sind auch die betroffenen Personen zu informieren;
- die Inanspruchnahme von Auftragsverarbeitern von personenbezogenen Daten unterliegt einem spezifischen Vertragsrahmen (vgl. obligatorische Klauseln);
- grenzüberschreitende Datenströme zu Nicht-EU-Ländern, die nicht als Länder anerkannt sind, die ein angemessenes Datenschutzniveau gewährleisten, sind unter Vorbehalt ausreichender Garantien, insbesondere Vertragsgarantien, möglich;
- alle Einrichtungen, die personenbezogene Daten erheben und verarbeiten, müssen folgende Verzeichnisse erstellen und regelmäßig aktualisieren:
 - ein Verzeichnis der Verarbeitungstätigkeiten personenbezogener Daten durch den für die Verarbeitung Verantwortlichen;
 - ein Verzeichnis der Verarbeitungstätigkeiten personenbezogener Daten durch den Auftragsverarbeiter;

Fokus - die Grundsätze und Verpflichtungen der Datenschutzpolitik in der Schweiz (Bundesdatenschutzgesetz):

Personendaten dürfen nur rechtmäßig bearbeitet werden. Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismäßig sein. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein. Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen. Die Personendaten müssen durch angemessene technische und organisatorische Maßnahmen gegen unbefugtes Bearbeiten geschützt werden.

4 Funktionen und Merkmale von SecuTix 360°

In diesem Abschnitt 4 wird Folgendes beschrieben:

- die zu erfüllenden Anforderungen und Verpflichtungen, wie in Abschnitt 3 oben erläutert;
- die Funktionen und Merkmale der Lösung SecuTix 360°, die Ihnen die Möglichkeit geben, diese Anforderungen und Verpflichtungen zu erfüllen.

4.1 Rechtmäßigkeit des Zwecks und der Verarbeitung der Daten

4.1.1 Grundsätze

Es ist Aufgabe des für die Datenverarbeitung Verantwortlichen, sich folgender Aspekte zu vergewissern:

- dass die Daten tatsächlich zu den festgelegten, eindeutigen und legitimen Zwecken erhoben werden und nicht später auf eine mit diesen Zwecken inkompatible Weise verarbeitet werden (vgl. Zweckbindungsgrundsatz);
- des rechtmäßigen Charakters der Datenerhebung und -verarbeitung im Rahmen der Lösung SecuTix 360° (vgl. Rechtmäßigkeitsgrundsatz).

Zur Erinnerung, die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- die betroffene Person hat sich mit der Verarbeitung ihrer personenbezogenen Daten zu einem oder mehreren spezifischen Zwecken einverstanden erklärt;
- die Verarbeitung ist für die Erfüllung des Vertrags erforderlich, den die betroffene Person abgeschlossen ist, oder für die Erfüllung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person ergriffen wurden;
- die Verarbeitung ist zur Einhaltung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
- die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich;

- die Verarbeitung ist für die Ausführung einer Aufgabe im öffentlichen Interesse erforderlich oder erfolgt in Ausführung öffentlicher Gewalt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;
- die Verarbeitung ist zu den rechtmäßigen Interessen erforderlich, die vom für die Verarbeitung Verantwortlichen oder einem Dritten wahrgenommen werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen, die diesen Schutz personenbezogener Daten fordern, insbesondere wenn die betroffene Person ein Kind ist.

4.1.2 Die Lösung SecuTix 360°

Die IT-Lösung SecuTix bietet folgende Funktionen:

- Ticketing-Management: Konfiguration, Planung, Reservierung, Verkauf, Ausgabe, Druck, Zugangskontrolle, Mitarbeiterverwaltung, ...
- Customer Relationship Management (Kunden und potenzielle Kunden): Marketingkampagnen, Kundenwerbe- und Aktionen zur Kundenansprache, diesbezügliche technische Vorgänge: Auswahl, Segmentierung, Datenanreicherung, gezielte Ansprache, E-Mailing, Analyse und Tracking (Webnavigation und E-Mailing), Berichte (Statistiken und Leistungen)
- Event-Management: Organisation, Planung, Referenten/Besucherführer, ...
- Verkaufsstellen- und Verkaufsmanagement: Bestandsaufnahme/Einkauf/Lieferantenmanagement.

Als für die Verarbeitung Verantwortlicher haben Sie sich für die Lösung SecuTix 360° als das Tool entschieden, das Ihrer Meinung nach am besten für die Verarbeitung personenbezogener Daten geeignet ist; der Zweck dieser Datenverarbeitung wurde von Ihnen selbst festgelegt. Es ist daher Ihre Aufgabe, sich zu vergewissern, dass die oben genannten Zweckbindungs- und Rechtmäßigkeitsgrundsätze eingehalten werden.

4.2 Verarbeitung nach Treu und Glauben und Transparenz der Datenerhebung und -verarbeitung

4.2.1 Grundsätze

Die betroffenen Personen müssen vom für die Datenverarbeitung Verantwortlichen über die Verarbeitung ihrer personenbezogenen Daten (vgl. Grundsatz der Verarbeitung nach Treu und Glauben und Transparenzgrundsatz) gemäß den geltenden Bestimmungen für den Schutz personenbezogener Daten informiert werden. Sie müssen darüber hinaus ihre Einwilligung gegeben haben (vgl. insbesondere Abschnitte 3.1, 4.3 und 4.9).

Weiterhin muss auf jedem Datenerfassungsformular ein Informationshinweis aufgeführt sein.

4.2.2 Die Lösung SecuTix 360°

Als für die Verarbeitung verantwortliche Person ist es daher Ihre Aufgabe, die betroffenen Personen wie oben erläutert zu informieren und ggf. ihre Einwilligung einzuholen. Wir stehen Ihnen selbstverständlich zur Verfügung, um Ihnen auf Anfrage die sich in unserem Besitz befindlichen Informationen mitzuteilen, die Ihnen diesbezüglich von Nutzen sein könnten.

Um Ihnen zu ermöglichen, Ihre diesbezüglichen Verpflichtungen einzuhalten, informieren wir Sie darüber hinaus, dass:

- SecuTix 360° auf seiner Web-Schnittstelle über eine Rubrik mit der Bezeichnung „Datenschutzerklärung“ verfügt, die auf allen Webseiten zugänglich ist und über einen Hypertext-Link auf eine Seite verweist, die Ihre Datenschutzerklärung oder -politik enthalten kann; für die Ausarbeitung des Inhalts dieser Erklärung oder Politik sind Sie selbst zuständig:

© 2014 SECUTIX | CRÉÉ PAR SECUTIX | CONDITIONS GÉNÉRALES DE VENTE | CHARTE DE CONFIDENTIALITÉ | FAQ

- Wenn Sie unser integriertes Web-Modul auf Ihrer Website benutzen, müssen Sie eine solche Rubrik in Ihre Website aufnehmen;
- Alle Online-Datenerhebungsformulare, die auf unserer Web-Schnittstelle und in unserem Web-Modul enthalten sind (wenn in Ihre Website integriert) weisen einen Rahmen auf, in dem Sie Ihren Datenschutzhinweis (für dessen Redaktion und Hosting Sie selbst zuständig sind), ein anzukreuzendes Feld für die Einwilligung und einen Link zu Ihrer Datenschutzerklärung (für dessen Redaktion und Hosting Sie selbst zuständig sind) aufführen können. Diese beiden Links werden über die Parameter der Internet-Verkaufsstellen festgelegt.

Darüber hinaus weisen wir Sie darauf hin, dass die Personen, die auf einem anderen Wege als über das Internet reservieren, ebenfalls informiert werden müssen. Folglich müssen Sie sich vergewissern, dass für jede Datenerhebungsart ein Informationsprozess gemäß den geltenden Datenschutzbestimmungen eingerichtet wird (zum Beispiel im Skript der Mitarbeiter in einem interaktiven Sprachserver bei der Datenerhebung per Telefon, durch Anzeige bei der Datenerhebung am Schalter etc.).

Auf jeden Fall müssen alle betroffenen Personen (verschiedene Kontakttypen, Mitarbeiter, Lieferanten, potenzielle Kunden, etc. deren Daten in SecuTix 360° erscheinen könnten) von Ihnen informiert werden und nicht nur die Personen, die eine Reservierung vornehmen. Daher ist es Ihre Aufgabe, sich der Einhaltung dieser Bestimmungen zu vergewissern und die diesbezüglichen Prozesse einzurichten.

4.3 Angemessenheit, Zweckdienlichkeit und strenge Notwendigkeit der Daten

4.3.1 Grundsätze

Die erhobenen und verarbeiteten Daten müssen dem Zweck angemessen und zweckdienlich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (vgl. Grundsatz der Datenminimierung).

Es geht darum, nur die Daten zu erheben und zu verarbeiten, die für den Zweck der Datenverarbeitung erforderlich sind (zum Beispiel für die Reservierung der Tickets, die Zuweisung der Plätze, die Zahlung der Bestellung, ...). Die Erhebung von nicht für den Zweck der Datenverarbeitung erforderlichen Daten muss für die betroffene Person fakultativ bleiben, wobei darauf hingewiesen wird, dass jegliche Datenerhebung, die nicht mit dem Zweck der Datenverarbeitung im Zusammenhang steht, streng untersagt ist.

Darüber hinaus ist es untersagt, bestimmte besonders sensible Daten zu erheben. Grundsätzlich sind die Erhebung und Verarbeitung folgender Daten untersagt:

- sog. „besondere“ Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
- Informationen zu Gesetzesverstößen, Verurteilungen oder entsprechenden Sicherheitsmaßnahmen (zum Beispiel „Stadionverbot“).

Es gibt allerdings Ausnahmen zu diesen Verboten. Zum Beispiel können die sog. „besonderen“ Daten verarbeitet werden, wenn sie unter den folgenden Annahmen für die Verarbeitung erforderlich sind:

- Einwilligung der betroffenen Person;
- Verarbeitung durch eine Stiftung, einen Verein oder eine andere gemeinnützige Einrichtung, die einen politischen, weltanschaulichen, religiösen oder gewerkschaftlichen Zweck verfolgt (unter bestimmten Bedingungen);
- Daten, die die betroffene Person offensichtlich öffentlich gemacht hat.

Diese Ausnahmen müssen jedoch streng ausgelegt werden.

Diese Grundsätze gelten unabhängig von den Bedingungen für die Erhebung, Erfassung und Verarbeitung der Informationen in den Tools. Insbesondere die Felder für freie Kommentare sind mit Vorsicht zu benutzen.

4.3.2 Die Lösung SecuTix 360°

Als für die Verarbeitung verantwortliche Person ist es Ihre Aufgabe dafür zu sorgen, dass diese Grundsätze der Datenminimierung und das Erhebungsverbot bestimmter Daten eingehalten werden.

Die Lösung SecuTix 360° bietet Ihnen Standarddatenerhebungsfelder, unabhängig davon, ob es sich um die Datenerhebung im Backoffice, auf der Ihnen zur Verfügung gestellten Web-Schnittstelle oder im Web-Modul handelt. Diese Felder sind im Hinblick auf eine Datenminimierung begrenzt. Es wird jedoch darauf hingewiesen, dass:

- es sich nur um einen Vorschlag für Standardfelder handelt, die Sie anpassen können (unter Vorbehalt bestimmter, zwingend vorgeschriebener Felder für den einwandfreien Betrieb der Lösung, die aber sehr begrenzt sind; zum Beispiel betreffen die einzigen obligatorischen Felder für die Kontakte die folgenden Daten: Anrede, Name und Vorname). Als für die Datenverarbeitung Verantwortlicher sind Sie für die Festlegung der zu benutzenden oder hinzuzufügenden Felder zuständig; Sie treffen diese Entscheidungen anhand der

Elemente, um deren Angabe wir Sie in Anhang 1 bitten, damit wir Ihre diesbezüglichen Anweisungen berücksichtigen können;

- das Gleiche gilt für die Festlegung der sog. im Rahmen der Segmentierungsfunktionen „berechneten“ Daten, die Sie zum Beispiel in Anhang 1 angeben können.

Die Lösung SecuTix 360° gibt Ihnen zwar Zugang zu den Segmentierungsfunktionen und eventuell auch zu den Profiling-Funktionen, dennoch entscheiden Sie allein über die Segmente, die Sie benutzen wollen, die verfolgten Zwecke, die Zweckdienlichkeit, die Eignung und die Notwendigkeit der in diesem Rahmen verarbeiteten Daten, die eventuellen bezüglich dieser Segmente zu treffenden Entscheidungen und die Folgen, die sich daraus für die betroffenen Personen ergeben könnten (und sind folglich auch dafür verantwortlich).

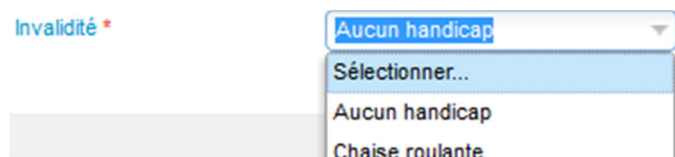
Es wird ebenfalls darauf hingewiesen, dass individuelle automatisierte Entscheidungen, zum Beispiel mittels Segmentierungs- oder Profiling-Funktionen besonderen Vorkehrungen unterliegen können, die von Ihnen zu beachten sind (Einwilligung, menschliches Eingreifen, Möglichkeit, die Entscheidung anzufechten, ...);

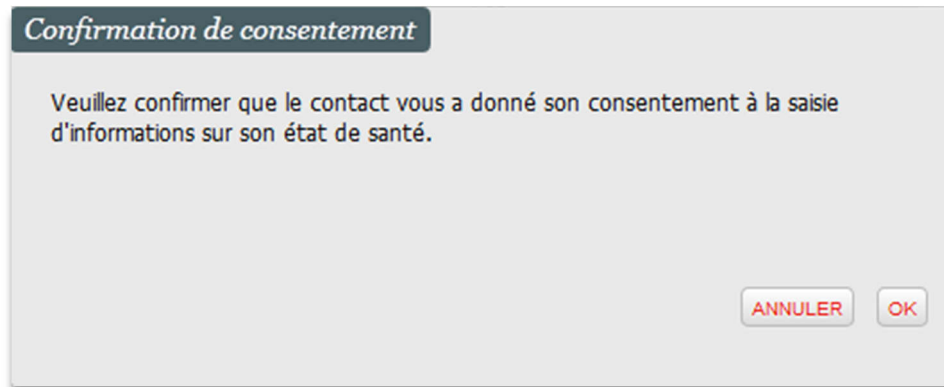
- die gleichen Regeln und Grundsätze für die Auswahl und Hinzufügung von Reporting- oder Extraktionskriterien anhand der Funktionen dieser Lösung gelten. Darüber hinaus wird angesichts der Risiken für die Daten aufgrund der Volatilität der Reportings oder Extraktionen nach ihrer Ausführung empfohlen, eine Autorisierungspolitik einzurichten, damit nur Personen, die diese Extraktionen wirklich vornehmen müssen, dazu befugt sind (in Anhang 1 anzugeben).

Die Lösung SecuTix 360° bietet Ihnen unter anderem bestimmte Funktionen, die es Ihnen ermöglichen, die für die Datenerhebung geltenden Grundsätze einzuhalten. Zum Beispiel:

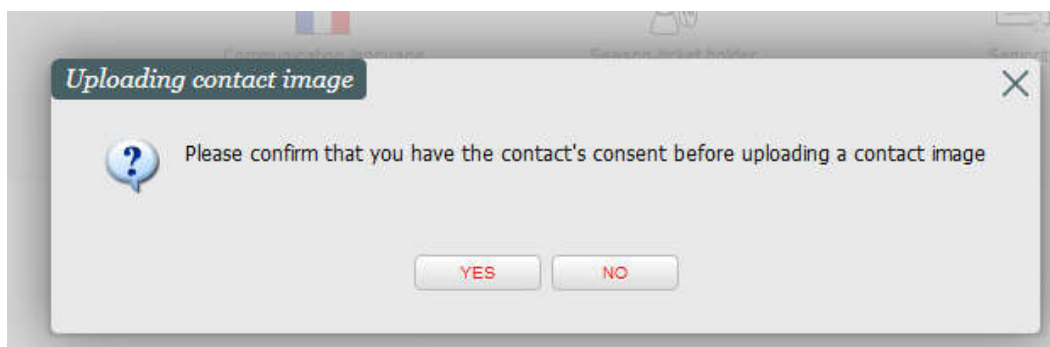
- der Standardwert für eine Behinderung ist „keine Behinderung“. Dieses Feld wird in Form eines Pull-Down-Menüs dargestellt, wodurch die Auswahl des Mitarbeiters bei der Eingabe der Information begrenzt wird und somit auch das Risiko, dass nicht unbedingt erforderliche Daten erhoben werden.

Um einen anderen Wert zu speichern, muss der Mitarbeiter Ihrer Einrichtung bestätigen, dass er die Einwilligung des Kontakts eingeholt hat, indem er das folgende Feld ankreuzt:





- um ein Foto zu speichern, muss der Mitarbeiter Ihrer Einrichtung bestätigen, dass er die Einwilligung des Kontakts eingeholt hat, indem er das folgende Feld ankreuzt:



Sie müssen diese Einwilligung ebenfalls einholen (in Ihrer Datenschutzerklärung), wenn Sie den Internetnutzern ermöglichen wollen, ein Foto online hochzuladen (vgl. über die Web-Schnittstelle oder das Web-Modul).

- Zahlkartendaten sind für die Mitarbeiter in der Lösung SecuTix 360° nicht vollständig zugänglich. Sie können jedoch codiert und gesichert nach einem Kauf durch einen Kontakt mit dessen Einwilligung gespeichert werden, zum Beispiel für spätere Einkäufe (ohne Kartenprüfnummer/Kryptogramm). Diese Speicherfunktion der Zahlkartendaten ist standardgemäß deaktiviert. Die Aktivierung dieser Funktion erfordert die Einwilligung der betroffenen Person, entweder:
 - indem die betroffene Person ein Feld auf der Web-Schnittstelle oder im Web-Modul ankreuzt (nicht im Voraus ausgewählt);
 - oder über ein im Backoffice der Lösung anzukreuzendes Feld (nicht im Voraus ausgewählt und mit dem verbindlichen Hinweis, ausdrücklich die Einwilligung des Kontakts einzuholen).

- bezüglich der freien Kommentarfelder in der Lösung muss der Mitarbeiter bei der Eingabe ein Feld ankreuzen, um zu bestätigen, dass der Kommentar mit den geltenden Datenschutzbestimmungen konform ist. Darüber hinaus gibt ein Link dem Mitarbeiter auf Wunsch zusätzliche Informationen:

Note > Nouveau

Note

Titre *

Placement

Ce monsieur a une préférence de placement en bas à droite de la salle.
Si possible lui proposer des places à cet endroit.

Je confirme que le commentaire saisi est conforme aux lois et règlements relatifs à la protection des données. Vous trouverez des recommandations [ici](#)

Recommandations relatives à la saisie des notes

Les données saisies dans des zones de commentaires libres doivent respecter les dispositions applicables en matière de protection des données à caractère personnel. Notamment, elles doivent :

- Etre pertinentes, adéquates, non excessives et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées et traitées ;
- Etre objectives, elles ne sauraient résulter d'un jugement de valeur ou d'une appréciation de comportement des intéressés (pour ce faire, vous êtes invité à rédiger les commentaires de manière factuelle, de type sujet - verbe - complément, en évitant les qualificatifs par exemple) ;
- Ne pas, directement ou indirectement, faire apparaître de données dites « particulières », qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, les informations relatives à des infractions, condamnations ou mesures de sûreté associées ;
- Bannir tous les termes ou expressions qui pourraient être considérés comme injurieux, péjoratifs, désobligeants, blessants ou attentatoires à la réputation, à la considération ou à la vie privée des personnes physiques.

FERMER

- bezüglich der freien Kommentarfelder auf der Web-Schnittstelle oder im Web-Modul bei der Beendigung der Bestellungen/Reservierungen/Optionen ist es Ihre Aufgabe, Ihre Mitarbeiter zu sensibilisieren und die erforderlichen Prozesse zum maßvollen Umgang mit diesen Kommentaren einzurichten. Weiterhin wird ein vereinfachter Warnhinweis für die Kontakte mit folgendem Standardtext eingefügt:

„Die in diesem Kommentarbereich eingegebenen Daten haben einzig und allein zum Ziel, die für die Erteilung und/oder Ausführung Ihrer Bestellung erforderlichen Elemente mitzuteilen. Wir weisen Sie darauf hin, dass die Informationen, die Sie uns in diesem freien Textfeld mitteilen, den Bestimmungen für den Schutz personenbezogener Daten unterliegen, zu deren Einhaltung Sie sich verpflichten (rechtmäßige, objektive, zweckdienliche, angemessene und auf das erforderliche Mindestmaß für den verfolgten Zweck beschränkte Daten, Datenerhebung und -verarbeitung nach Treu und Glauben etc.).“

- die Bildschirme der Lösung zur Erstellung von Reports oder Abfragen enthalten einen Warnhinweis für die Nutzer der Lösung:

„Wenn Sie diese Daten exportieren, müssen Sie sich vergewissern, dass Sie im Einklang mit den geltenden Grundsätzen zum Schutz personenbezogener Daten handeln. Sie müssen sich insbesondere vergewissern, dass die Datei, die erstellt wird, nur im Rahmen der ursprünglichen Verarbeitung und insbesondere für den

gleichen Zweck wie in dieser Anwendung vorgesehen benutzt wird. Sie müssen sich darüber hinaus vergewissern, dass die extrahierten Daten maßgeblich, angemessen und für den Zweck erforderlich sind, für den Sie ihre Nutzung vorgesehen haben, und dass die Daten nur befugten Personen mitgeteilt werden. Es ist Ihre Aufgabe, darauf zu achten, dass alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit und insbesondere der Geheimhaltung getroffen werden. Die Exportdatei darf nicht über die Frist, die für im Rahmen dieser Anwendung verarbeitete Daten vorgesehen ist, hinaus gespeichert werden“.

4.4 Nutzung von Cookies auf der Web-Schnittstelle oder im Web-Modul

4.4.1 Grundsätze

SecuTix 360° ermöglicht die Analyse des Verhaltens der Internetnutzer über die Lösung Google Analytics. Diese Funktion zur Besuchermessung und Erstellung von Besucher- und Navigationsstatistiken kann entweder von Ihrer Einrichtung oder von SecuTix SA eingesetzt werden, um den Service zu verbessern.

Der Internetnutzer muss darüber informiert werden, dass Google Analytics Cookies verwendet, und sich mit ihrer Speicherung und Nutzung einverstanden erklären.

Dazu muss der Internetnutzer, der die Website besucht (Startseite oder nachfolgende Seiten), durch ein Banner über Folgendes informiert werden:

- genaue Zwecke der verwendeten Cookies;
- Möglichkeit, sich gegen diese Cookies auszusprechen und die Parameter durch Anklicken eines Links im Banner zu ändern (dieser Link muss zu einer Cookie-Richtlinie weiterleiten, in der die Internetnutzer auf einfache und verständliche Weise über die Lösungen informiert werden, die ihnen zur Verfügung stehen, um einen Teil oder die Gesamtheit der Cookies zu akzeptieren oder abzulehnen);
- die Tatsache, dass bei der Fortsetzung der Navigation auf der Website Cookies auf seinem Datenendgerät abgelegt werden.

Da die Einwilligung eindeutig sein muss, muss dieses Banner solange angezeigt werden, wie die Person ihre Navigation nicht fortgesetzt hat, das heißt, solange sie keine weitere Seite der Website aufgerufen hat oder auf kein weiteres Element der Website geklickt hat (Bild, Link, Schaltfläche „Suchen“).

Außer bei vorheriger Einwilligung des Internetnutzers dürfen keine einer Einwilligung unterliegenden Cookies auf seinem Datenendgerät abgelegt oder gelesen werden:

- wenn der Internetnutzer die Website öffnet und seine Navigation nicht fortsetzt: Die Untätigkeit des Nutzers darf nicht als Willensäußerung angesehen werden;
- wenn er auf den Link im Banner klickt, um die Cookies zu parametrieren und ggf. die Ablage von Cookies ablehnt.

Und schließlich müssen die Personen, die ihre Einwilligung zur Ablage oder zum Lesen von Cookies erteilt haben, die Möglichkeit haben, diese jederzeit aufzuheben. Bei Einwilligung der betroffenen Person wird diese nach Ablauf von 13 Monaten erneut um ihre Einwilligung gebeten (vgl. maximale Nutzungsdauer der Cookies).

Zur Information: Es gibt Ausnahmen zur Notwendigkeit, die Einwilligung für Cookies zur Besuchermessung einzuholen, wenn folgende Bedingungen erfüllt sind:

- der Internetnutzer ist darüber informiert (vgl. Banner);
- er hat die Möglichkeit, Cookies mittels eines leicht zu benutzenden Widerspruchsverfahrens für alle Datenendgeräte, Betriebssysteme, Anwendungen und Webbrowser abzulehnen; Informationen zu Personen, die ihr Widerspruchsrecht geltend machen, dürfen nicht erhoben und dem Herausgeber des Besucheranalysetools übermittelt werden;
- der Zweck der Vorrichtung muss auf die Besuchermessung des eingesehenen Inhalts beschränkt sein, um eine Bewertung der veröffentlichten Inhalte und der Ergonomie der Website oder der Anwendung zu ermöglichen;
- die erhobenen Daten dürfen nicht mit anderen Verarbeitungen kombiniert werden (zum Beispiel Kundendateien oder Besucherstatistiken anderer Websites); die Nutzung des verwendeten Cookies muss streng auf die Erstellung anonymer Statistiken beschränkt sein; das Ausmaß muss auf einen einzigen Herausgeber beschränkt sein und darf keine Verfolgung der Navigation der Person ermöglichen, die verschiedene Anwendungen nutzt oder auf verschiedenen Websites navigiert;
- die Nutzung der IP-Adresse zur Geolokalisierung des Internetnutzers darf keine weiteren Angaben als die Stadt liefern; diese IP-Adresse muss nach der Geolokalisierung sofort gelöscht oder anonymisiert werden, um eine weitere Nutzung dieser Daten oder eine Zusammenführung mit anderen personenbezogenen Daten zu vermeiden;
- da es sich um Cookies handelt, darf ihre Nutzungsdauer dreizehn Monate nicht überschreiten; diese Dauer muss automatisch bei jedem neuen Besuch einer Website verlängert werden; die über die Cookies erhobenen Informationen dürfen maximal dreizehn Monate gespeichert werden.

4.4.2 Die Lösung SecuTix 360°

Als Herausgeber einer Website (unabhängig davon, ob Sie unsere Web-Schnittstelle oder unser in Ihre eigene Website integriertes Web-Modul verwenden) ist es Ihre Aufgabe, die Einwilligung der Internetnutzer bezüglich der Ablage und des Lesens von Cookies einzuholen und sie darüber zu informieren.

Diesbezüglich setzen wir Sie darüber hinaus in Kenntnis, dass:

- Ihnen unsere Support-Abteilung auf Anfrage die Anzeige eines Informationsbanners zur Einholung der Einwilligung zwecks Installation von Cookies beim ersten Besuch eines Internetnutzers auf unserer Web-Schnittstelle und in unserem Web-Modul anbietet. Für die Formulierung der an den Internetnutzer gerichteten Information über dieses Banner sind Sie zuständig. Wir schlagen Ihnen jedoch folgende Formulierung vor, die Sie an die jeweiligen Anforderungen Ihrer eigenen Website anpassen oder entsprechend abändern können:

Wenn Sie die Navigation auf dieser Website fortsetzen, akzeptieren Sie die Nutzung von Cookies oder ähnlichen Technologien, die die Erstellung von Besucherstatistiken auf unserer Website (Tests und Messungen der Besucherzahlen, Besuchshäufigkeit, Navigation, Leistung) zum Ziel haben, aber auch **[ggf. durch andere Zwecke je nach Web-Schnittstelle zu ergänzen]**.

Wenn Sie mehr darüber erfahren und Ihre Cookies und ähnlichen Technologien parametrieren wollen, klicken Sie hier **[Link zur Cookie-Richtlinie einfügen]**.

Ein solches Banner muss auf jeden Fall eingerichtet werden, unabhängig davon, ob Sie unsere Web-Schnittstelle oder unser in Ihre Website integriertes Web-Modul verwenden. Dieses Banner muss auf der ersten Seite der Website eingerichtet werden, auf die der Internetnutzer trifft, selbst wenn es sich um eine sekundäre Seite und nicht um die Startseite handelt;

- Sie sind für die Beschreibung der „Cookie-Richtlinie“ zuständig. Wir weisen Sie jedoch darauf hin, dass wir im Rahmen unserer Web-Schnittstelle folgende Cookies verwenden:

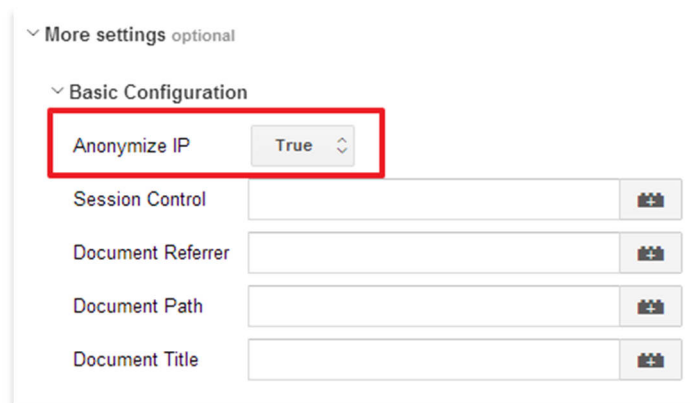
Typ	Name	Herausgeber	Zwecke	Dauer
Permanente Cookies dienen zu Statistikzwecken und zur Messung der Besucherzahlen und Häufigkeit der Besuche	_ga	Google Inc. (Google Analytics)	<p>Wenn Google Analytics aktiviert ist, werden diese Cookies auf der Grundlage der bei der Navigation des Nutzers gesammelten Informationen eingesetzt, insbesondere die URL-Adresse, von der der Nutzer auf die Website zugreift, der Internetprovider des Nutzers, die Art, die Konfiguration und die Parametrierung des Browsers, ...</p> <p>Diese Cookies dienen dazu, die einmaligen Besucher einer Website zu unterscheiden, indem ihnen eine nach dem Zufallsprinzip generierte Nummer als Nutzer-ID zugewiesen wird. Diese Nutzer-ID wird bei jeder angesehenen Seite aktualisiert und dient insbesondere dazu, die Anzahl der Besuche, Sessions, etc. zu berechnen ...</p> <p>Weitere Informationen finden Sie unter: https://support.google.com/analytics/answer/6004245 Deaktivierungsmodul von Google Analytics: https://support.google.com/analytics/answer/181881?hl=fr&ref_topic=2919631. ou https://tools.google.com/dlpage/gaoptout.</p>	Je nach Parametrierungsentscheidungen des Kunden
Session-Cookie	lang		Dieser Cookie zeichnet die Sprachauswahl des Kontakts auf.	Session
Session-Cookie mit	SESSION		Technische ID der Session	Session





technischem Zweck				
Session-Cookie mit technischem Zweck	BIGipServer_XXX		Dieser Cookie ermöglicht die Weiterleitung des Kontakts zur gleichen Maschine im Hinblick auf die Nutzung von Caching-Optionen.	Session
Session-Cookie mit technischem Zweck	AcpAT_XXX		Dieser Cookie dient dazu zu validieren, dass der Kontakt einwandfrei über PeakProtect hergestellt wurde (Managementtool für hohe Besucherzahlen)	Session

Diese Informationselemente müssen von Ihnen in Ihre Cookie-Richtlinie eingefügt werden.

Eine solche Cookie-Richtlinie muss auf jeden Fall eingerichtet werden, unabhängig davon, ob Sie unsere Web-Schnittstelle oder unser in Ihre Website integriertes Web-Modul verwenden;

- grundsätzlich gilt, dass Cookies nicht installiert werden, solange der Internetnutzer seine Navigation nicht fortgesetzt hat; das Banner muss nach Ablauf von 13 Monaten ab Erhalt der Einwilligung für die Nutzung von Cookies erneut angezeigt werden. Diese Konfiguration wird standardmäßig auf Web-Schnittstellen vorgeschlagen, die von SecuTix SA nach einer diesbezüglichen Serviceanfrage Ihrerseits zur Verfügung gestellt werden. Sie müssen sich vergewissern, dass diese Verpflichtung auf Ihrer eigenen Website eingehalten wird, auch wenn Sie unser in Ihre Website integriertes Modul benutzen;
- wenn Sie sich der Einwilligungsverpflichtung entziehen wollen (damit die Cookies schon auf der Startseite installiert werden können), müssen Sie die Cookies gemäß den oben erläuterten Grundsätzen parametrieren, da Cookies zur Messung der Besucherzahlen keiner Einwilligung unterliegen. Insbesondere (aber nicht ausschließlich) muss ein Mitarbeiter Ihrer Einrichtung Google Analytics so konfigurieren, dass die IP-Adressen vor dem Versand der Daten an Google in den USA anonymisiert werden, damit keine Zusammenführung mit anderen personenbezogenen Daten möglich ist:



More settings optional
 Basic Configuration
 Anonymize IP True
 Session Control 
 Document Referrer 
 Document Path 
 Document Title 

Darüber hinaus müssen Sie die anderen Verpflichtungen bezüglich der Ausnahmeregelungen zu dieser Einwilligung einhalten.

Achtung, diese Ausnahmeregelungen zur Einwilligung gelten nur für Cookies zur Messung der Besucherzahlen: Die Nutzung von anderen Cookies wie Cookies in den sozialen Netzwerken oder Werbe-Cookies unterliegen weiterhin der vorherigen Zustimmung des Internetnutzers.

4.5 Speicherdauer der Daten

4.5.1 Grundsätze

Die Bestimmungen zum Schutz personenbezogener Daten sehen vor, dass die Daten nur für eine Dauer gespeichert werden dürfen, die mit den verfolgten Zwecken im Verhältnis steht. Die Bestimmungen enthalten jedoch keine Angaben zur genauen Speicherdauer. Die unbegrenzte Speicherung von personenbezogenen Daten ist auf jeden Fall nicht zulässig.

4.5.2 Die Lösung SecuTix 360°

Als für die Verarbeitung Verantwortlicher ist es Ihre Aufgabe, die maximale Speicherdauer der Daten in den Tools, die Sie für die Verarbeitung personenbezogener Daten verwenden, und insbesondere in der Lösung SecuTix 360° festzulegen und anzuwenden. Diese maximale Speicherdauer betrifft alle Personen, deren Daten in der Lösung SecuTix 360° erhoben und verarbeitet werden.

Die Lösung SecuTix 360° bietet mehrere Funktionen, die Ihnen ermöglichen, diese Daten zu löschen:

- die Kontakte, die über ein persönliches Online-Konto verfügen, haben die Möglichkeit, ihre Daten in diesem Konto zu löschen:



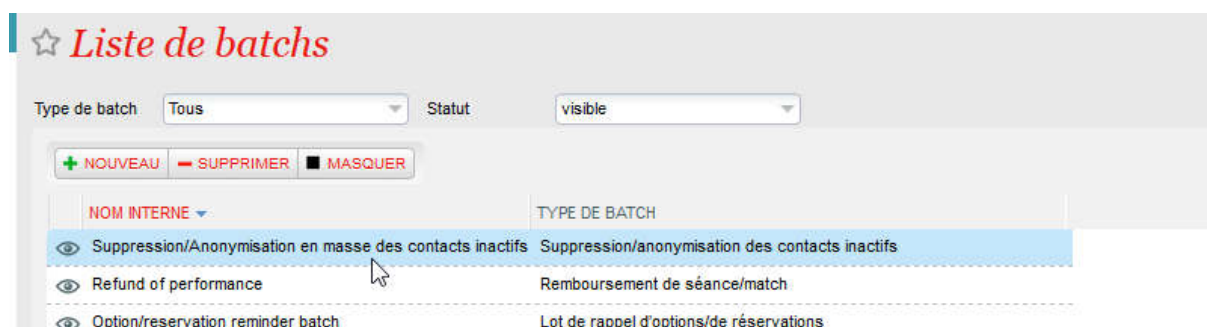
- die Mitarbeiter Ihrer Einrichtung haben die Möglichkeit, Kontakte zu löschen:



- in diesen beiden Fällen werden das Konto des Kontakts sowie die Marketinginformationen (Historie und Indikatoren) gelöscht und alle Bestellungen werden anonymisiert. Die Anonymisierung der Daten ist nach dem Löschen der

Logs nicht wieder rückgängig zu machen, das heißt nach einer Frist von 12 Monaten (vgl. Speicherdauer der Logs);

- die Mitarbeiter Ihrer Einrichtung haben die Möglichkeit, potenzielle Kunden zu löschen;
- die Mitarbeiter Ihrer Einrichtung haben die Möglichkeit, manuell die Daten aller betroffenen Personen zu anonymisieren;
- SecuTix 360° stellt Ihnen darüber hinaus eine Funktion zur Verfügung, die es Ihnen je nach Ihren Entscheidungen, Praktiken, Ihrem Aktivitätssektor und den für Sie geltenden Bestimmungen ermöglicht, seit X Monaten inaktive Kontakte zu erheben und sie zusammen zu löschen/anonymisieren:



- Nachdem Sie ein Mitarbeiterkonto in den Zustand „ausgesetzt“ versetzt haben, können Sie es anonymisieren, indem Sie Angaben wie Name/Vorname/E-Mail/etc. durch XXXX ersetzen. Die Anonymisierung der Daten ist nach dem Löschen der Logs nicht wieder rückgängig zu machen, das heißt nach einer Frist von 12 Monaten (vgl. Speicherdauer der Logs). Achtung, Sie können das Login der Benutzer nicht ändern/anonymisieren. Daher ist es Aufgabe der Administratoren, die diese Benutzerprofile erstellen, keine Informationen einzugeben, anhand derer die Person identifiziert werden kann.

Nach Ablauf des Vertrags werden Ihre Daten extrahiert und Ihnen in einem marktüblichen Standardformat übergeben. Sie werden dann aus der SecuTix Lösung gelöscht und folgen den gleichen Regeln wie beim manuellen Löschen (siehe oben).

4.6 Korrekte, aktualisierte Daten. Recht auf Zugang, Berichtigung, Löschung und Übertragbarkeit. Recht auf Einschränkung der Verarbeitung und Widerspruchsrecht gegen Verarbeitung

4.6.1 Grundsätze

Gemäß den für den Schutz personenbezogener Daten geltenden Bestimmungen müssen die verarbeiteten Daten korrekt sein und ggf. aktualisiert werden. Der für die Verarbeitung Verantwortliche hat alle angemessenen Maßnahmen zu treffen, damit Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Den betroffenen Personen muss ein Recht auf Zugang, Berichtigung, Löschung und Übertragbarkeit ihrer Daten gewährt werden.

Darüber hinaus haben diese Personen ein Recht auf Einschränkung der Verarbeitung sowie ein Widerspruchsrecht gegen die Verarbeitung ihrer Daten.

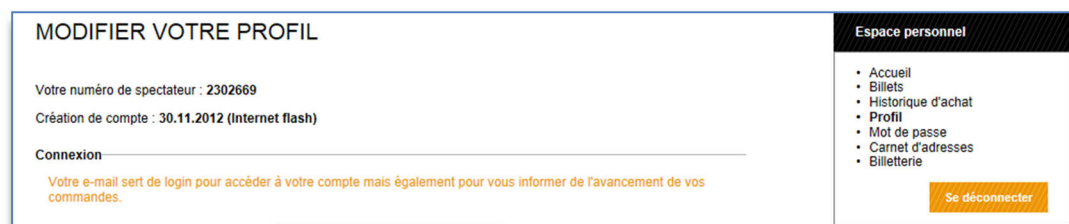
Für die Einhaltung dieser Verpflichtungen ist der für die Verarbeitung Verantwortliche zuständig. Der Auftragsverarbeiter muss den für die Verarbeitung Verantwortlichen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der vorgenannten Rechte der betroffenen Person nachzukommen.

4.6.2 Die Lösung SecuTix 360°

Als für die Verarbeitung Verantwortlicher müssen Sie sich vergewissern, dass Sie den betroffenen Personen die in den geltenden Bestimmungen vorgesehenen Antworten liefern, wenn diese Personen ihre vorgenannten Rechte ausüben, und dass ihren Anfragen (unter dem Vorbehalt, dass sie die entsprechenden Voraussetzungen erfüllen) Folge geleistet wird. Diesbezüglich wird darauf hingewiesen, dass wir, wenn eine Anfrage direkt an uns gerichtet wird, Sie darüber informieren. Allerdings sind Sie weiterhin für die Beantwortung der Anfrage und die sich daraus ergebenden Aktionen zuständig.

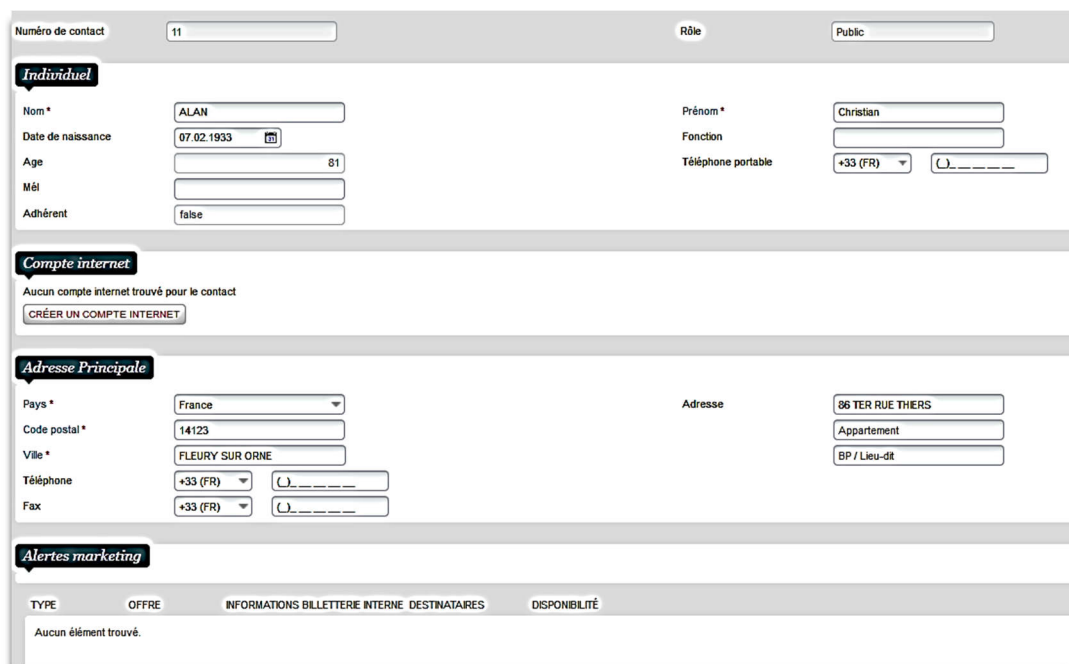
SecuTix 360° bietet Funktionen für die Verwaltung von Anfragen zur Berichtigung oder Löschung von Daten, die in der SecuTix 360° Datenbank gespeichert sind.

- die Internetnutzer können die Daten ihres Profils jederzeit online in ihrem persönlichen Online-Konto ändern:



The screenshot shows a user profile management interface. The main content area is titled 'MODIFIER VOTRE PROFIL' and contains the following information: 'Votre numéro de spectateur : 2302669', 'Création de compte : 30.11.2012 (Internet flash)', and a 'Connexion' field. A note below the connection field states: 'Votre e-mail sert de login pour accéder à votre compte mais également pour vous informer de l'avancement de vos commandes.' On the right side, there is a sidebar titled 'Espace personnel' with a menu: 'Accueil', 'Billets', 'Historique d'achat', 'Profil', 'Mot de passe', 'Carnet d'adresses', and 'Billetterie'. A 'Se déconnecter' button is located at the bottom right of the sidebar.

- die Mitarbeiter Ihrer Einrichtung können die Kontaktdatenblätter aktualisieren:



The screenshot displays a contact management form. At the top, there are fields for 'Numéro de contact' (value: 11) and 'Rôle' (value: Public). The form is divided into several sections:

- Individuel:** Fields for 'Nom *' (ALAN), 'Prénom *' (Christian), 'Date de naissance' (07.02.1933), 'Age' (81), 'Mél', 'Adhérent' (false), and 'Fonction'.
- Compte internet:** A message 'Aucun compte internet trouvé pour le contact' and a 'CRÉER UN COMPTE INTERNET' button.
- Adresse Principale:** Fields for 'Pays *' (France), 'Code postal *' (14123), 'Ville *' (FLEURY SUR ORNE), 'Adresse' (86 TER RUE THIERS), 'Appartement', 'BP / Lieu-dit', 'Téléphone' (+33 (FR)), and 'Fax' (+33 (FR)).
- Alertes marketing:** A table with columns: TYPE, OFFRE, INFORMATIONS BILLETTERIE INTERNE DESTINATAIRES, and DISPONIBILITÉ. The table is currently empty, showing 'Aucun élément trouvé.'

- zu den Datenlöschungsanfragen siehe Abschnitt 4.5.

Ein Kontakt kann darum bitten, dass ihm alle seine personenbezogenen Informationen im Rahmen der Ausübung seines Rechts auf Zugang oder Übertragbarkeit seiner Daten mitgeteilt werden. Die Mitarbeiter Ihrer Einrichtung haben Zugang zu den Daten der Kontakte, um dieser Anfrage nachzukommen. Auf Anfrage an SecuTix SA kann ein Mitarbeiter Ihrer Einrichtung auch alle zu einem Kontakt gespeicherten Informationen erhalten (Kontaktdatenblatt, Kaufhistorie, Beziehungshistorie).

Darüber hinaus:

- ist die Herkunft der Informationen auf dem Kontaktdatenblatt als „vom Internetnutzer eingegebene Informationen“, „von einem Mitarbeiter Ihrer Einrichtung eingegebenen Informationen“ oder als „durch Datenimport erhobene Informationen“ angegeben:

Contact > 13 Monsieur REMI ALEXIS (Prospect)

Résumé Général Marketing Gestion Notes Administration

Créé au moyen de	IMPORT	Créé le	20.12.2012
Créé par	IMPCTCT_demostr	Modifié le	07.01.2014
Modifié par	STX-41025-pre		

- ist das Erstellungsdatum eines persönlichen Kontos im besagten Konto angegeben:

Modifier votre profil

Votre numéro de spectateur : 203017

Création de compte : 09.08.2012 (Internet grand public)

Connexion

Votre e-mail sert de login pour accéder à votre compte mais également pour vous informer de l'avancement de vos commandes.

- sind das Erstellungsdatum eines Kontaktdatenblatts und das Datum der letzten Änderung im Kontaktdatenblatt angegeben:

Contact > 13 Monsieur REMI ALEXIS (Prospect)

Résumé Général Marketing Gestion Notes Administration

Créé au moyen de	IMPORT	Créé le	20.12.2012
Créé par	IMPCTCT_demostr	Modifié le	07.01.2014
Modifié par	STX-41025-pre		

Und schließlich ist es Ihre Aufgabe, in der Lösung die Anfragen zur Einschränkung der Datenverarbeitung oder auf Widerspruch gegen die Datenverarbeitung zu verwalten.

Wir verpflichten uns, alles zu tun, um Ihnen auf Anfrage die Elemente in unserem Besitz zu übermitteln, damit Sie die Anfrage der betroffenen Personen auf Ausübung ihrer Rechte zufriedenstellend beantworten können.

4.7 Datensicherheit

4.7.1 Grundsätze

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen unter anderem Folgendes ein:

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Es ist Ihre Aufgabe, Maßnahmen zur Sicherheit und Geheimhaltung der Daten zu treffen. Empfehlungen zur Datensicherheit finden Sie unter: <https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>.

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen.

Darüber hinaus muss der für die Verarbeitung Verantwortliche bei Verletzung des Schutzes personenbezogener Daten (Verstoß gegen die Sicherheit, der unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung, Veröffentlichung oder zum unerlaubten Zugang zu den personenbezogenen Daten führt, die Gegenstand der Verarbeitung sind) die zuständigen Aufsichtsbehörden unverzüglich und wenn möglich spätestens innerhalb von 72 Stunden informieren, nachdem er von diesem Verstoß Kenntnis erlangt hat. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, muss der Verantwortliche die betroffene Person unverzüglich über die Verletzung informieren.

4.7.2 Die Lösung SecuTix 360°

Als für die Verarbeitung Verantwortlicher ist es Ihre Aufgabe dafür zu sorgen, dass alle diese Verpflichtungen eingehalten werden.

Als Auftragsverarbeiter ist SecuTix SA verpflichtet, angemessene Sicherheitsmaßnahmen zu ergreifen, den für die Verarbeitung Verantwortlichen unverzüglich nach Kenntnisnahme über eine Verletzung des Schutzes personenbezogener Daten zu informieren und allgemein mit dem für die Verarbeitung Verantwortlichen zusammenzuarbeiten, damit letzterer seinen eigenen Verpflichtungen nachkommen kann (insbesondere Umsetzung angemessener Sicherheitsmaßnahmen und Auswirkungsanalyse).

SecuTix SA gewährleistet, die Anforderungen der Norm ISO/IEC 27001:2013 und PCI DSS v3.2 zu erfüllen und die entsprechenden Konformitätszertifikate erhalten zu haben. Daher verpflichtet sich SecuTix SA, alle in diesen Normen aufgeführten technischen und organisatorischen Maßnahmen zu ergreifen.

Darüber hinaus gilt für die Lösung SecuTix 360°:

- Die Daten werden in Echtzeit auf mehreren redundanten Festplatten dupliziert.
- Die Daten werden fast in Echtzeit in zwei, mehrere Kilometer voneinander entfernten Datacenter dupliziert.
- Um die Server und die Lösung angemessen zu sichern, ergreift SecuTix SA alle erforderlichen technischen und organisatorischen Maßnahmen, insbesondere Zugangskontrolle, Einsatz einer Firewall und eines aktuellen Anti-Virus-Programms, SSL-Codierung und Journale/Logs, wenn Bankdaten manuell geändert werden.
- Der Teil in SecuTix 360°, der die Bezahlung betrifft, ist nach PCI DSS zertifiziert und wird einmal pro Jahr einem Audit unterzogen.
- Die Passwörter müssen eine sichere Buchstaben- und Ziffernkombination in ausreichender Zahl aufweisen, um gültig zu sein.
- SecuTix 360° verfügt über einen Kontinuitätsplan, um von einem Datacenter zum anderen umschalten zu können.
- Die physischen Zugänge der Personen zu den Datacentern werden streng per Code, Rückverfolgung, Alarm, Ausweiskarten und Videoüberwachung kontrolliert.
- Die an den Ersatzstandort gesandten Daten werden via VPN oder HTTPS codiert.

Darüber hinaus verpflichten wir uns im Einklang mit unseren Verpflichtungen, mit Ihnen im Hinblick auf folgende Aspekte zusammenzuarbeiten:

- Einhaltung Ihrer Verpflichtungen in Bezug auf die Sicherheit und den Schutz personenbezogener Daten durch Ihre Einrichtung;
- Durchführung von Auswirkungsanalysen der Verarbeitung von personenbezogenen Daten durch Ihre Einrichtung, wenn die Art der Verarbeitungen, an denen wir beteiligt sind, dies erfordert, und ggf. einer eventuellen Konsultation der Aufsichtsbehörde zu diesen Datenverarbeitungen.
- Einhaltung Ihrer Melde- und Informationsverpflichtung bei der Aufsichtsbehörde im Falle von Verletzungen des Schutzes personenbezogener Daten. Zu diesem Zweck melden wir Ihnen alle Verletzungen des Schutzes personenbezogener Daten, von denen wir Kenntnis erlangen. Wir verpflichten uns ebenfalls, Ihnen auf Ihre Anfrage die erforderlichen Dokumente in unserem Besitz zu übermitteln, damit Sie ggf. die vorgenannten Meldungen vornehmen können, falls sich diese als notwendig erweisen sollten.

Darüber hinaus müssen Sie in Ihrer Einrichtung die geeigneten technischen und organisatorischen Maßnahmen treffen, um zur Erreichung eines angemessenen Sicherheitsniveaus der im Rahmen der Lösung SecuTix 360° verarbeiteten Daten beitragen. Daher empfehlen wir Ihnen zum Beispiel:

- die aktuellen Zugänge zu SecuTix 360° zu schützen (Hardware, Software, Netz, Internetzugang);
- die Geheimhaltung der Passwörter zu gewährleisten, mit denen sich die Mitarbeiter Ihrer Einrichtung bei SecuTix 360° anmelden, und darauf zu achten, dass eine Passwortpolitik gemäß den geltenden Empfehlungen einrichtet wird (vgl. zum Beispiel die unter dem nachstehenden Link einsehbaren Empfehlungen: <https://www.cnil.fr/fr/authentication-par-mot-de-passe-les-mesures-de-securite-elementaires>);
- das Antivirus-Programm auf allen Arbeitsplätzen regelmäßig zu aktualisieren;
- ...

4.8 Auftragsverarbeiter, Unterauftragsverarbeiter und grenzüberschreitende Datenströme

4.8.1 Grundsätze

Die Inanspruchnahme von Auftragsverarbeitern und/oder Sub-Auftragsverarbeitern zur Verarbeitung personenbezogener Daten unterliegt einem spezifischen Vertragsrahmen, der eine Reihe von obligatorischen Klauseln umfasst.

Die grenzüberschreitenden Datenströme zu Nicht-EU-Ländern, die nicht als Länder anerkannt sind, welche ein angemessenes Datenschutzniveau gewährleisten, sind unter Vorbehalt ausreichender Garantien, insbesondere Vertragsgarantien, möglich.

4.8.2 Die Lösung SecuTix 360°

Im Rahmen der Bereitstellung der Lösung SecuTix 360° für den Einsatz in Ihrer Einrichtung kann es vorkommen, dass wir als Auftragsverarbeiter in Ihrem Namen personenbezogene Daten für Sie verarbeiten müssen. Die Vertragsdokumente, die wir Ihnen vorschlagen, enthalten eine mit den Anforderungen der DSGVO konforme Klausel, die zum Ziel hat, unsere Leistungen als Auftragsverarbeiter von personenbezogenen Daten in Ihrem Namen zu regeln.

Im Hinblick auf die Lieferung dieser Lösung können die verschiedenen Einheiten unserer Gruppe ebenfalls personenbezogene Daten in Ihrem Namen verarbeiten. Diesbezüglich setzen wir Sie darüber in Kenntnis, dass die Geschäftseinheiten unserer Gruppe im Wesentlichen in der Europäischen Union oder in der Schweiz niedergelassen sind, das heißt in Ländern, die ein angemessenes Datenschutzniveau aufweisen. Eine Geschäftseinheit ist jedoch in Vietnam ansässig. Gemäß den geltenden Datenschutzbestimmungen sind die grenzüberschreitenden Datenströme zu dieser Einheit durch eine Vereinbarung für grenzüberschreitende Datenströme geregelt, die auf der Grundlage der Schweizer Modelle des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und der Modelle der Europäischen Kommission ausgearbeitet wurde.

Darüber hinaus kann es vorkommen, dass wir, um Ihnen alle im Rahmen der Lösung SecuTix 360° angebotenen Funktionen bereitstellen zu können, je nach Leistungen und Services, deren Erbringung Sie bei uns abgeschlossen haben, die Tätigkeit von Unterauftragsverarbeitern in Anspruch nehmen, deren Liste Sie in Anhang 2 finden.

4.9 Nutzung von Daten zu Marketingzwecken

4.9.1 Grundsätze

Für die Nutzung von Daten zu Marketingzwecken gelten folgende Grundsätze:

- Erfordernis einer ausdrücklichen Einwilligung (positiv ausgedrücktes Opt-in mittels eines nicht im Voraus angekreuzten Kästchens) für die Kommunikation per E-Mail, SMS, MMS, Fax oder ein automatisiertes elektronisches Kommunikationssystem (vgl. zum Beispiel automatisches Anrufsystem);
- kein vorheriger Widerspruch gegen die Kommunikation per E-Mail oder Telefon mit menschlicher Beteiligung;
- jede Sendung (insbesondere E-Mail und SMS) muss ein einfaches und kostenloses Mittel enthalten, um die Kommunikation auf diesem Wege zu deaktivieren (Widerspruchsrecht), sowie Erfordernis für Sendungen auf elektronischem Wege, einen Betreff in Verbindung mit dem Inhalt und Informationen über den Anzeigenkunden anzugeben, für den sie versandt werden.

Bezüglich der Sendungen per E-Mail, SMS oder MMS ist anzugeben, ob eine Ausnahme zur Einwilligung unter dem Vorbehalt geltend gemacht werden kann, dass alle folgenden Voraussetzungen erfüllt sind:

- die Kontaktdaten des Empfängers wurden bei ihm selbst anlässlich eines Verkaufs oder einer Serviceleistung erhoben;
- Einhaltung der geltenden Bestimmungen zum Schutz personenbezogener Daten, insbesondere Information der Personen;

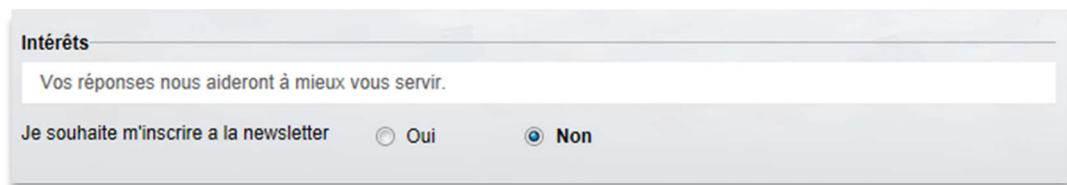
- die direkte Kundenwerbung betrifft analoge Produkte oder Serviceleistungen zu denen, die von der gleichen juristischen oder natürlichen Person geliefert wurden;
- der Empfänger erhält die ausdrückliche und unmissverständliche Möglichkeit, kostenlos - mit Ausnahme der Kosten für die Übermittlung des Widerspruchs - und einfach Widerspruch gegen die Nutzung seiner Kontaktdaten zu dem Zeitpunkt einzulegen, zu dem sie erhoben werden, und jedes Mal, wenn ihm eine E-Mail zu Kundenwerbungszwecken gesandt wird.

4.9.2 Die Lösung SecuTix 360°

SecuTix 360° bietet Ihnen Marketingfunktionen, mit denen Sie Ihren Kontakten (Kunden und potenziellen Kunden) Werbenachrichten senden können. Sie haften jedoch allein für die Nutzung dieser Funktionen und müssen die oben erläuterten Grundsätze einhalten.

Damit Sie Ihre Marketingaktionen gemäß den oben erläuterten Grundsätzen durchführen können, hat SecuTix SA folgende Funktionen eingerichtet:

- Das Online-Formular für die Erstellung eines persönlichen Kontos durch einen Internetnutzer über unsere Web-Schnittstelle oder unser Web-Modul enthält einen Rahmen mit einem Informationshinweis, dessen Inhalt Sie selbst festlegen. Dieser Hinweis muss von Ihnen mit anzukreuzenden Kästchen (nicht im Voraus angekreuzt) und den vorgeschriebenen Informationen zur Einwilligung/zur Widerspruchsmöglichkeit ergänzt werden. Diese Elemente werden in der „Internet-Verkaufsstelle“ parametrierbar;
- die Internetnutzer verfügen standardmäßig über mehrere Funktionen in ihrem persönlichen Online-Konto, wie zum Beispiel:
 - Anmeldung/Abmeldung für Newsletter (kann an Ihre Erfordernisse angepasst werden):



- Auswahl der Kommunikationsmedien und der Absender (kann an Ihre Erfordernisse angepasst werden):

	J'accepte	Je refuse
Je souhaite recevoir par mail toute l'actualité: calendrier des événements, alertes de mise en vente, nouveautés, exclusivités. *	<input type="radio"/>	<input checked="" type="radio"/>
Je souhaite recevoir par SMS des offres exclusives. *	<input type="radio"/>	<input checked="" type="radio"/>
J'accepte que mes coordonnées soient transmises à des tiers partenaires. *	<input type="radio"/>	<input checked="" type="radio"/>

- am Schalter (im Backoffice):
 - ein Mitarbeiter Ihrer Einrichtung kann festlegen, ob ein Kontakt Mitteilungen von Ihrer Einrichtung, Partnern Ihrer Einrichtung oder Dritten erhält:

Informations légales

Accepte communication de l'organisme oui non

Accepte transmission des coordonnées élec. à des tiers oui non

Accepte communication d'un partenaire oui non

- ein Mitarbeiter kann die vom Kontakt gewünschten Kommunikationskanäle festlegen:

Communication

Canal de communication préféré

Moment préféré

SMS_MMS oui non

Téléphone oui non

Mél oui non

Courrier oui non

- Als Standard ist keine Option ausgewählt. Die Auswahl einer Option erfordert daher eine „positive“ Aktion von Seiten des Internetnutzers oder des Mitarbeiters. Bei der Durchführung Ihrer Marketingaktionen gemäss den in Abschnitt 4.9.1 erläuterten Grundsätzen müssen Sie diese Regeln beachten.

Darüber hinaus müssen Sie die Widerspruchsanfragen in Bezug auf Kundenwerbung berücksichtigen, die Ihnen von den betroffenen Personen je nach Kommunikationskanal zur Kenntnis gebracht werden (Ankreuzen von „Nein“ für die Kommunikationskanäle).

Zur Sensibilisierung der Nutzer der Lösung umfasst SecuTix 360° einen Warnhinweis auf den Bildschirmen zur Durchführung von Kundenwerbungsaktionen mit folgendem Wortlaut:

„Bezüglich der von Ihnen geplanten Kundenwerbungsaktionen weisen wir Sie darauf hin, dass Sie folgende Grundsätze beachten müssen:

- *Es ist untersagt, einen Kontakt über einen Kommunikationskanal anzusprechen, für den „Nein“ angekreuzt ist;*
- *die Kundenwerbung per E-Mail, SMS, MMS, Fax oder ein automatisiertes elektronisches Kommunikationssystem ist nur möglich, wenn „Ja“ für den Kommunikationskanal angekreuzt ist;*

- *die Kundenwerbung per Post oder Telemarketing ist nur möglich, wenn „Ja“ für den Kommunikationskanal angekreuzt ist (oder wenn weder „Ja“ noch „Nein“ angekreuzt ist).“*

Die von SecuTix 360° auf Ihre Anfrage versandten Newsletter umfassen mindestens Informationen, die den Empfängern ermöglichen, ihr Widerspruchsrecht auszuüben (d. h. ihren Wunsch, keine solchen Sendungen mehr zu erhalten). In den Mitteilungen ermöglicht ein Link, den Versand abzubestellen. Die Abmeldung wird automatisch in SecuTix 360° berücksichtigt (Feld „Nein“ angekreuzt):

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

Um diese Funktion in den Versand Ihrer E-Mails zu integrieren, müssen Sie eine der beiden nachstehenden Möglichkeiten in die Konfiguration Ihrer zu versendenden E-Mails aufnehmen:

- in der versandten E-Mail konfiguriert der Mitarbeiter Ihrer Einrichtung den Link „Unsubscribe URL“. Die Abmeldung erfolgt automatisch, wenn der Kontakt den Link anklickt:

Unsubscribe URL <https://citm-daysoff.shop.secutix.com/api/1/redirect/unsubscribe?id=xEjA2Zzp1h75YxnCB%2FV9yP1qDbw%3D>

- in der versandten E-Mail fügt der Mitarbeiter Ihrer Einrichtung einen Link ein, der den Kontakt zu seinem persönlichen Bereich weiterleitet. Der Kontakt kann dort sein Abonnement abbestellen oder seine Präferenzen ändern.

4.10 Formalitäten

4.10.1 Grundsätze

Jeder Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen.

Jeder Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

Diese Verzeichnisse sind schriftlich zu führen; dies kann auch in einem elektronischen Format erfolgen. Der Verantwortliche oder der Auftragsverarbeiter stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

4.10.2 Die Lösung SecuTix 360°

Als für die Verarbeitung Verantwortlicher müssen Sie die Verarbeitung personenbezogener Daten im Rahmen der Lösung SecuTix 360° in Ihr Verzeichnis „für die Verarbeitung Verantwortlicher“ der Verarbeitungstätigkeiten eintragen.

Als Auftragsverarbeiter tragen wir alle Verarbeitungen personenbezogener Daten im Rahmen der Lösung SecuTix 360°, die wir in Ihrem Auftrag ausführen, in unser Verzeichnis „Auftragsverarbeiter“ der Verarbeitungstätigkeiten ein.

Anhang 1. Von Ihrer Einrichtung auszufüllende Checkliste zur Verarbeitung personenbezogener Daten in der Lösung SecuTix 360°

Frage	Antwort
Nutzungszwecke der Lösung und der vertraglich abgeschlossenen Leistungen/Services	Verfolgte Ziele, gewählte Anwendungsfunktionalitäten, tatsächliche oder geplante Verwendungen, Zwecke, die den spezifischen Bestimmungen entsprechen, Folgen der Verarbeitung,....
In der Lösung erhobene und verarbeitete Daten	... Angaben zu den Daten, die der Kunde bei der Nutzung der SecuTix 360°-Lösung erheben und verarbeiten möchte.
Personen, die befugt sind, neue Felder hinzuzufügen, und Bedingung für die diesbezüglichen Anfragen bei SecuTix SA	Die Identität der autorisierten Personen beim Kunden mitteilen + angeben, wie die Anfragen an SecuTix SA gestellt werden können.
Personen, die befugt sind, neue Segmentierungskriterien hinzuzufügen, und Bedingung für die diesbezüglichen Anfragen bei SecuTix SA	Die Identität der autorisierten Personen beim Kunden mitteilen + angeben, wie die Anfragen an SecuTix SA gestellt werden können.
Personen, die befugt sind, neue Reporting-/Extraktionskriterien hinzuzufügen, und Bedingung für die diesbezüglichen Anfragen bei SecuTix SA	Die Identität der autorisierten Personen beim Kunden mitteilen + angeben, wie die Anfragen an SecuTix SA gestellt werden können.
Empfänger von "Administrator"-Identifikatoren	Es liegt dann in der Verantwortung des Kunden, selbst die Personen zu bestimmen und zu konfigurieren, die Zugriff auf die Daten haben, sowie die Details der Berechtigungen für die Daten, Bildschirme, Funktionalitäten (z.B.: Beratung, Eingabe, Reporting / Extraktion,....).
Gewünschte Speicherdauer der Daten in der Lösung	Die SecuTix 360° Lösung bietet eine Shelf Life Management Funktionalität, die dem Kunden die Möglichkeit gibt, die gewünschte Haltbarkeit selbst einzustellen.
Kontakt in der Einrichtung für Anfragen zur Ausübung der Rechte durch die betroffenen Personen	Übermittlung der Identität und Kontaktinformationen an den Kunden
Kontakt in der Einrichtung bei Verstoß gegen den Schutz personenbezogener Daten	Übermittlung der Identität und Kontaktinformationen an den Kunden

Datenschutzbeauftragte

Geben Sie die Identität und die Kontaktdaten des Datenschutzbeauftragten des Kunden oder zumindest des Referenten für den Schutz personenbezogener Daten an.

Weitere Anweisungen der Organisation an die SecuTix AG

Spezifizieren Sie alle anderen Anweisungen des Kunden zu Händen von SecuTix SA.

Anhang 2. Liste der Unterauftragsverarbeiter von SecuTix SA

Name	Aktivität	Land	Transferierte personenbezogene Daten
Amazon Web Services	Hosting von öffentlichen Dateien	USA	Nein
Google Maps for Work	Standardisierung, Validierung und automatischer Vorschlag von Postanschriften	USA	Nein
Pca Predict	Standardisierung, Validierung und automatischer Vorschlag von Postanschriften	UK	Nein
Ingenico ePayment	Zahlungsdienstleister	Frankreich/Belgien	Ja
Datatrans	Zahlungsdienstleister	Schweiz	Ja
Orange Business Services – Contact Everyone	SMS-Routing	Frankreich	Ja
Maxmind	Geolokalisierung von IP-Adressen	USA	Ja
EFSTA	Steuerbescheinigungen	Österreich	Ja
Nazaries	Kundendienst	Spanien	Ja
SecuTix SA	Vertriebshändler, Kundendienst	Frankreich	Ja
SecuTix Iberia S.L.	Vertriebshändler	Spanien	Ja
SecuTix Ltd	Vertriebshändler	UK	Ja
Elca Informatique SA	Softwareentwicklung, Onboarding von Neukunden, Kundendienst, Betrieb und Wartung, Hosting	Schweiz	Ja
Elca Spanien	Softwareentwicklung und -integration, Kundendienst	Spanien	Ja
Elca Information Technology Ltd	Softwareentwicklung, Onboarding von Neukunden, Kundendienst, Betrieb und Wartung	Vietnam	Ja
Eric David	Softwareentwicklung, Support, Onboarding	Schweiz	Ja
Agorasophia Edutainment Spa Management	Vertrieb und Onboarding	Italien	Ja
Swantegy USA LLC	Vertrieb und Onboarding	USA	Ja
Softjourn, Inc	Vertrieb und Onboarding	USA	Nein