Cahier de protection des données

Date	08 Février 2018
Auteur	MKM / FLO
Réviseur	CPF
Version	2.1

Table des matières

1 Introduction

En tant qu'organisme utilisant la solution SecuTix 360°, vous recueillez et traitez en qualité de responsable de traitement des données personnelles concernant notamment vos clients acheteurs de billets, vos prospects, vos opérateurs,… Ces données peuvent également être transmises et/ou traitées par SecuTix SA, en qualité de sous-traitant, pour les besoins de la fourniture de cette solution et des prestations ou services que vous avez souscrits auprès de nous.

Dans le cadre de la collecte, du traitement et de la transmission de ces données personnelles, vous devez respecter la règlementation applicable en matière de protection des données personnelles. Le respect des exigences qui vous sont applicables en matière de protection des données relève, en votre qualité de responsable de traitement, de votre seule responsabilité.

En Union européenne (UE), la règlementation applicable est issue d'un règlement européen, le règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (dit « RGPD »), applicable directement dans tous les pays membres de l'UE à compter du 25 mai 2018.

SecuTix SA est soumise à la législation suisse sur la protection des données (voir encart ci-dessous). Cette législation est très similaire, voire sur certains points identique, à celle des pays de l'Union Européenne (UE). Par décision de la Commission européenne (décision de la Commission 2000/518 CE du 26.07.2000), la Suisse a d'ailleurs été reconnue comme assurant un niveau adéquat de protection des données à caractère personnel transférées depuis l'UE.

Aussi, SecuTix SA met à votre disposition une solution qui vous permet de respecter les exigences européennes en la matière. Ci-dessous nous vous montrons, sans prétention d'exhaustivité, les possibilités techniques et organisationnelles offertes par SecuTix 360° à cette fin.

Précisions liminaires

A titre liminaire, il est précisé que :

- le présent cahier de protection des données a uniquement vocation à vous présenter les fonctionnalités offertes par la solution SecuTix 360° dans une optique de sensibilisation et d'information s'agissant des précautions prise par nos soins afin de vous permettre de respecter certaines exigences légales ou réglementaires qui pourraient vous être applicables en votre qualité de responsable de traitement ;
- ce document ne constitue en aucune mesure des instructions à votre attention ou des conseils à vocation juridique ;
- la détermination des finalités et des moyens du traitement relève de vos seules décisions et relève de votre seule responsabilité, vos instructions devant d'ailleurs nous être transmises au moyen de la check-list figurant en Annexe 1.

2 Définitions

Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou social (syn. dans le présent document « données personnelles ») ;

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

Responsable de traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre (syn. dans le présent document « vous », « votre organisme ») ;

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (syn. dans le présent document « nous », « SecuTix SA ») ;

Personne concernée : personne physique dont les données à caractère personnel font l'objet d'un traitement dans le cadre de l'utilisation de la solution SecuTix 360° ;

Violation de données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

3 Exigences règlementaires

La règlementation européenne impose à tout responsable de traitement le respect des principes suivants :

- la collecte et le traitement des données doivent répondre aux principes de licéité, de loyauté et de transparence ;
- la finalité du traitement des données doit être déterminée, explicite et légitime. Les données personnelles ne doivent pas être traitées ultérieurement de manière incompatible avec cette finalité ;
- les données collectées et traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies. Elles doivent être exactes et mises à jour. Les données présentant une certaine sensibilité ne

peuvent être collectées et traitées que sous certaines conditions, notamment avec le consentement des personnes concernées ;

- la durée de conservation des données ne doit pas être excessive mais au contraire strictement proportionnée à la (ou aux) finalité(s) poursuivie(s) ;
- les personnes concernées doivent être informées du traitement de leurs données personnelles, et le cas échant leur consentement recueilli pour certains traitements. L'information à porter à la connaissance desdites personnes concernées doit contenir un certain nombre de mentions obligatoires ;
- les personnes concernées doivent se voir garantir un droit d'accès, de rectification, d'effacement et de portabilité de leurs données, ainsi qu'un droit à la limitation et un droit d'opposition au traitement desdites données. Elles disposent également du droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques les concernant ou les affectant de manière significative de façon similaire ;
- des mesures techniques et organisationnelles doivent être déployées pour assurer la sécurité des données, et notamment leur protection contre tout accès ou toute destruction, altération ou diffusion non autorisés desdites données (une analyse d'impact étant dans certaines hypothèses nécessaire pour évaluer les mesures adéquates à déployer, ce dont il peut résulter une obligation de consultation de l'autorité de contrôle compétente). Les violations de données à caractère personnel doivent par ailleurs faire l'objet d'un processus spécifique de notification auprès de l'autorité de contrôle compétente, voire d'une information des personnes concernées dans certaines hypothèses ;
- le recours à des sous-traitants et à des sous-traitants ultérieurs pour le traitement des données à caractère personnel doit faire l'objet d'un encadrement contractuel spécifique (cf. clauses obligatoires) ;
- les flux transfrontières de données vers des Etats non membres de l'UE et non reconnus comme assurant un niveau de protection adéquate des données peuvent être mis en œuvre sous réserve de garanties suffisantes, notamment contractuelles ;
- tout organisme collectant et traitant des données à caractère personnel doit élaborer et tenir à jour :
  - un registre de ses activités de traitement de données à caractère personnel mises en œuvre en qualité de responsable de traitement ;
  - un registre de ses activités de traitement de données à caractère personnel mises en œuvre en qualité de sous-traitant.

Focus - les principes et engagements sur la protection des données en Suisse (Loi fédérale sur la protection des données) :

Tout traitement de données doit être licite. Leur traitement doit être effectué conformément aux principes de la bonne foi et de la proportionnalité. Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite. Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées.

4 Fonctionnalités et caractéristiques de SecuTix 360°

Ce paragraphe 4 décrit :

- les exigences et obligations à respecter, telles que rappelées au paragraphe 3 supra ;
- les fonctionnalités et caractéristiques de la solution SecuTix 360° vous donnant la possibilité de vous y conformer.

4.1 Légitimité de la finalité et licéité du traitement des données

4.1.1 Principes

Il appartient au responsable de traitement de s'assurer :

- que les données sont effectivement collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités (cf. principe de finalité) ;
- du caractère licite de la collecte et du traitement des données au sein de la solution SecuTix 360° (cf. principe de licéité).

Pour mémoire, un traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

4.1.2 La solution SecuTix 360°

La solution informatique SecuTix 360°propose les fonctionnalités suivantes :

- gestion de la billetterie : configuration, planification, réservation, vente, émission, impression, contrôle d'accès, gestion des opérateurs,…
- gestion des relations de contact (clients et prospects) : campagnes marketing, opérations de prospection et de sollicitation, opérations techniques associées : sélection, segmentation, enrichissement des données, ciblage, emailing, analytique & tracking (navigation web et emailing), rapports (statistiques et performances))
- gestion d'événements : organisation, planification, conférenciers / guides,…
- gestion des magasins et des ventes : inventaire / achat / gestion des fournisseurs.

En tant que responsable de traitement, vous avez fait le choix de la solution SecuTix 360° comme le moyen selon vous le plus adéquat pour réaliser le traitement de données à caractère personnel dont la finalité, déterminée par vos soins, vous est propre. Il vous appartient de vous assurer que les principes précités de finalité et de licéité sont respectés.

4.2 Loyauté et transparence de la collecte et du traitement des données

4.2.1 Principes

Les personnes concernées doivent être informées par le responsable de traitement des traitements mis en œuvre concernant leurs données à caractère personnel (cf. principe de loyauté et de transparence), conformément aux dispositions applicables en matière de protection des données à caractère personnel. Elles doivent par ailleurs, dans certains cas, y avoir consenti (cf. paragraphes 3.1, 4.3 et 4.9 notamment).

En outre, une mention d'information doit figurer sur tout formulaire de collecte de données.

4.2.2 La solution SecuTix 360°

En votre qualité de responsable de traitement, il vous appartient donc d'informer les personnes concernées comme précité, voire de recueillir leur consentement. Nous nous tenons bien entendu à votre disposition pour vous fournir sur demande les informations en notre possession qui vous seraient utiles à cette fin.

Par ailleurs, pour vous permettre de respecter vos obligations en ce sens, nous vous informons que :

- SecuTix 360° intègre dans son interface web, une rubrique intitulée « Charte de confidentialité », accessible depuis toutes les pages web, renvoyant par un lien hypertexte vers une page pouvant contenir votre charte ou politique de protection des données, le contenu de cette charte ou politique devant être élaboré par vos soins :

- si vous utilisez notre module web intégré dans votre site internet, il conviendra d'intégrer sur votre site internet une telle rubrique ;
- tous les formulaires de collecte en ligne figurant dans notre interface web et dans notre module web (si intégré dans votre site internet) comportent un encadré vous permettant d'intégrer votre mention d'information confidentialité (dont la rédaction et l'hébergement vous appartiennent), une case à cocher de recueil du consentement, et un lien vers votre Charte de confidentialité (dont la rédaction et l'hébergement vous appartiennent). Ces deux liens sont renseignés via les paramètres des points de vente Internet.

En outre, nous vous rappelons que les personnes qui réservent par un autre moyen qu'une réservation web doivent de même être informées. Par conséquent, il convient que vous vous assuriez que pour chaque mode de collecte des données, un processus d'information conforme aux dispositions applicables en matière de protection des données est déployé (par exemple, dans le script des opérateurs ou dans un serveur vocal interactif en cas de collecte de données par téléphone, par affichage en cas de collecte de données au guichet, etc.).

En tout état de cause, toutes les personnes concernées (différents types de contacts, opérateurs, fournisseurs, prospects,… dont les données pourraient figurer dans la solution SecuTix 360°) devront être informées par vos soins, et non uniquement les personnes qui procèdent à une réservation. Aussi, il vous appartient de vous en assurer et de déployer les processus en ce sens.

4.3 Pertinence, adéquation et stricte nécessité des données

4.3.1 Principes

Les données collectées et traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies (cf. principe de minimisation des données collectées).

Il s'agit de ne collecter et traiter que les données nécessaires à la finalité du traitement (par exemple, pour la réservation des billets, l'attribution des places, le paiement de la commande,…). La collecte de données non indispensables à la finalité du traitement doit rester facultative pour la personne concernée, étant précisé que toute collecte de données sans rapport avec la finalité du traitement est strictement interdite.

Par ailleurs, un certain nombre de données particulièrement sensibles ne doivent pas être collectées. En effet, sont par principe interdits la collecte et le traitement des données suivantes :

- les 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 (par exemple, "interdiction de stade").

Il existe des exceptions à ces interdictions. A titre d'exemple, les données dites « particulières » peuvent être traitées si elles dont nécessaires au traitement dans les hypothèses suivantes :

- consentement de la personne concernée ;
- traitement effectué par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale (sous certaines conditions) ;
- données manifestement rendues publiques par la personne concernée.

Toutefois, ces exceptions doivent être interprétées de manière stricte.

Ces principes s'appliquent quelles que soient les modalités de collecte, de saisie et de traitement de l'information dans les outils. Les champs de commentaires libres doivent notamment être utilisés avec prudence.

4.3.2 La solution SecuTix 360°

En votre qualité de responsable de traitement, il vous appartient de vous assurer du respect de ces principes de minimisation des données et d'interdiction de collecte de certaines données.

La solution SecuTix 360° vous propose des champs de collecte de données par défaut, que ce soit dans le back-office ou dans l'interface ou module web mis à votre disposition. Ces champs sont limités dans une optique de minimisation des données. Toutefois, il est rappelé que :

- il ne s'agit que de champs proposés par défaut que vous pouvez ajuster (sous réserve de certains champs strictement obligatoires pour le bon fonctionnement de la solution mais qui sont très limités ; à titre d'exemple, les seules données strictement obligatoires dans la solution s'agissant des contacts sont les données suivantes : civilité, nom et prénom). En qualité de responsable de traitement, la détermination des champs à utiliser voire à ajouter vous revient, conformément aux éléments que nous vous demandons de compléter en Annexe 1 pour nous faire part de vos instructions en ce sens ;
- il en est de même s'agissant de la définition des données dites « calculées » dans le cadre des fonctionnalités de segmentation par exemple, que vous pouvez choisir de spécifier en Annexe 1.

  A cet égard, si la solution SecuTix 360° vous donne accès à des fonctionnalités de segmentation et éventuellement de profilage, vous êtes seul décisionnaire (et donc seul responsable) des segments que vous souhaitez utiliser, des finalités poursuivies, de la pertinence, de l'adéquation et du caractère nécessaire des données traitées dans ce cadre, des décisions que vous seriez éventuellement

amené à prendre au regard de ces segments et des conséquences pouvant en résulter pour les personnes concernées.

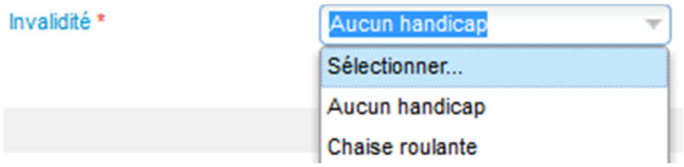
Il est également rappelé que la prise de décisions individuelles automatisées au moyen par exemple de fonctionnalités de segmentation voire de profilage peut être soumise à des précautions particulières qu'il vous appartient de respecter (consentement, intervention humaine, possibilité de contestation de la décision,…) ;

- les mêmes règles et principes sont applicables au choix et à l'ajout de critères de reportings ou d'extractions à partir des fonctionnalités de la solution. Par ailleurs, compte tenu des risques pour les données, liés à la volatilité des reportings ou extractions une fois réalisés, il est recommandé de mettre en place une politique d'habilitations n'autorisant que les personnes qui y ont strictement intérêt à pouvoir procéder à des extractions (à préciser en Annexe 1).

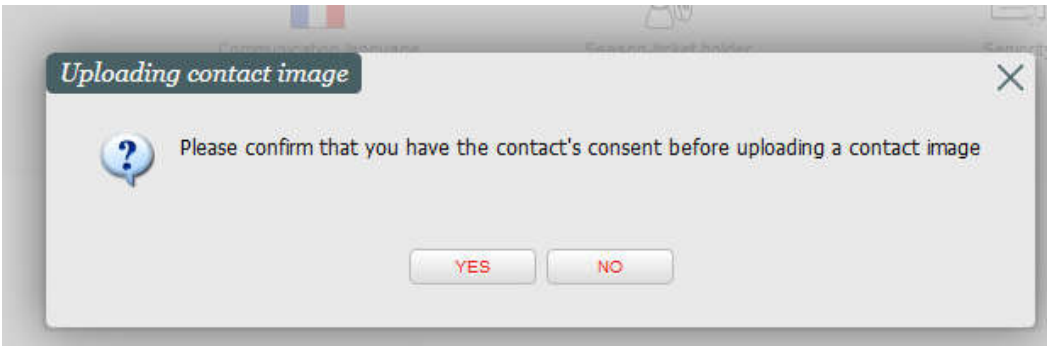
La solution SecuTix 360° vous propose en outre certaines fonctionnalités visant à vous permettre de respecter les principes applicables s'agissant des données collectées. A titre d'exemple :

- la valeur par défaut pour un handicap est « Aucun handicap ». Par ailleurs, ce champ est présenté sous la forme d'un menu déroulant limitant le choix de l'opérateur lors de la saisie de l'information afin de limiter les risques que des données non strictement nécessaires soient collectées.

  Pour enregistrer une autre valeur, l'opérateur de votre organisme doit confirmer qu'il a demandé le consentement au contact en cochant une case comme suit :



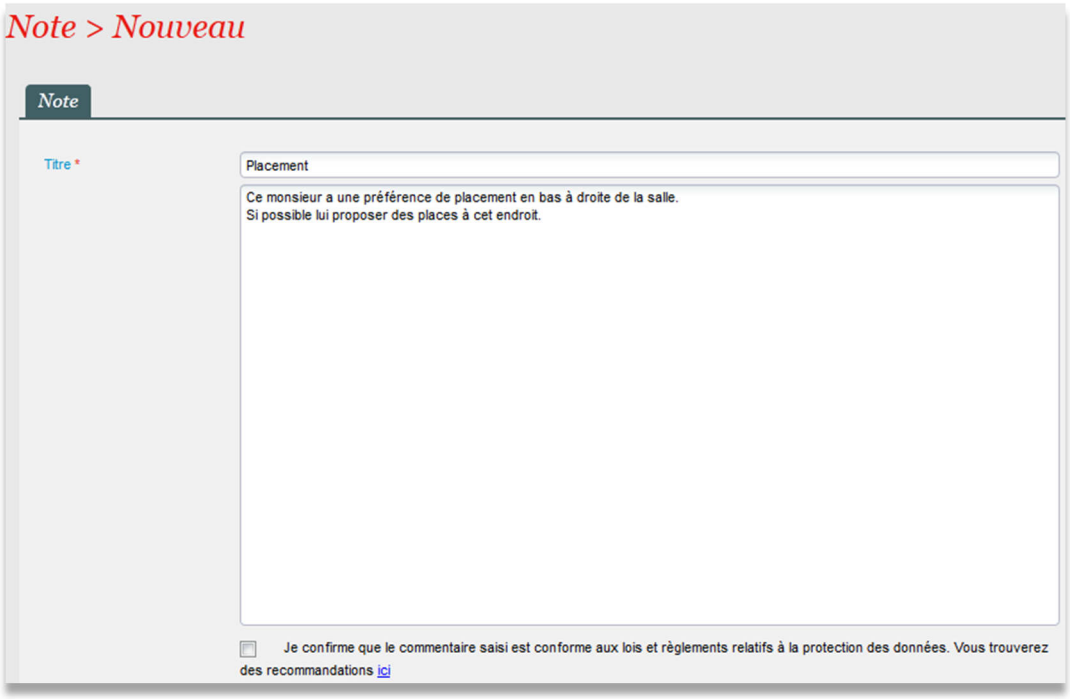
- pour enregistrer une photographie, l'opérateur de votre organisme doit confirmer qu'il a demandé le consentement au contact en cochant une case comme suit :

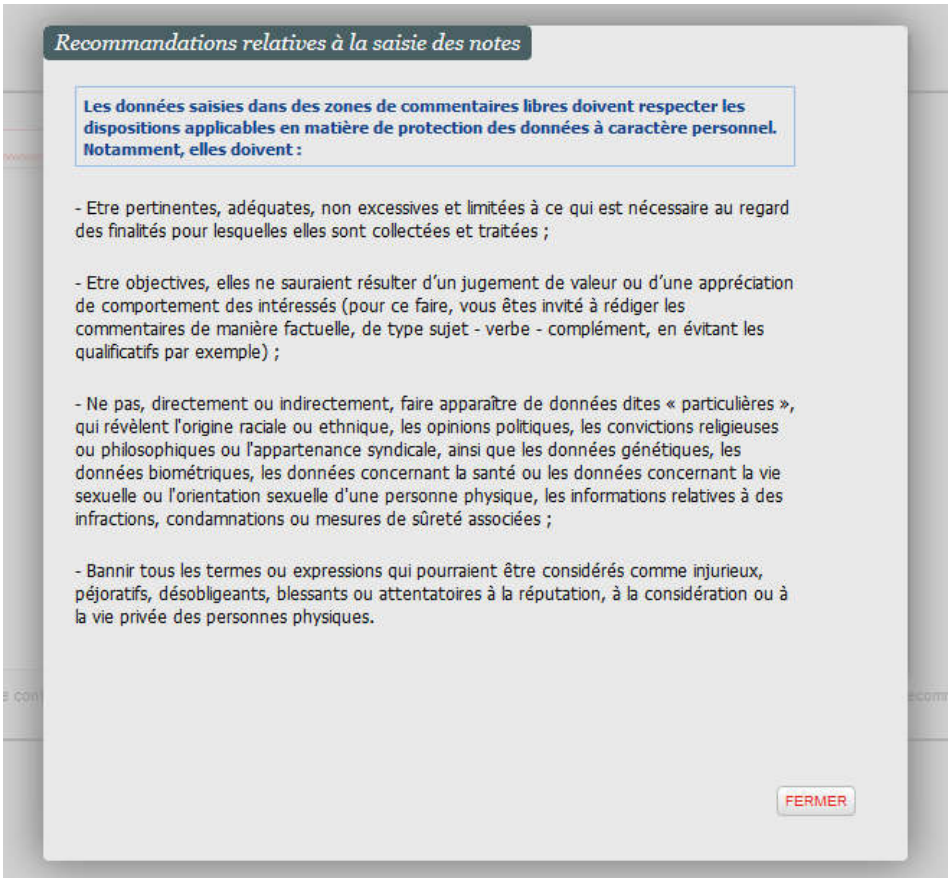


Il vous appartient également de prévoir le recueil de ce consentement (dans votre Charte de Confidentialité) lorsque vous choisissez de permettre aux internautes d'uploader leur photographie en ligne (cf. via l'interface ou le module web).

- les données de carte de paiement ne sont pas accessibles « en clair » par les opérateurs dans la solution SecuTix 360°. Toutefois, elles peuvent être conservées de manière chiffrée et sécurisée, suite à un achat effectué par un contact, avec le consentement de ce dernier, par exemple en vue de la réalisation d'achats ultérieurs (hors CVV / cryptogramme). Par défaut, cette fonctionnalité de conservation des informations de carte de paiement est désactivée. L'activation de cette fonctionnalité nécessite le consentement de la personne concernée, que ce soit :
  - au moyen d'une case à cocher par la personne concernée dans l'interface ou le module web (non pré-cochée) ;
  - au moyen d'une case à cocher dans le back-office de la solution (non pré-cochée et avec mention de l'obligation de demander le consentement explicite du contact).

- pour ce qui concerne les zones de commentaires libres figurant dans la solution, au moment de la saisie, l'opérateur de votre organisme doit cocher une case pour confirmer que le commentaire est conforme aux dispositions applicables en matière de protection des données à caractère personnel. De plus, un lien donne une information supplémentaire à l'opérateur s'il désire plus d'informations, comme suit :





- pour ce qui concerne les zones de commentaires libres de l'interface ou module web proposés lors de la finalisation des commandes/reservations/options, il vous

revient de mettre en place la sensibilisation aux opérateurs et les processus nécessaires à la modération de ces commentaires. En outre, une mention d'avertissement simplifié à l'attention des contacts est insérée avec le texte par défaut :

> *« Les données saisies dans cette zone de commentaires ne doivent avoir pour objectif que de préciser des éléments strictement nécessaires à la passation et/ou à l'exécution de votre commande. Par ailleurs, nous vous rappelons que les informations que vous pourrez communiquer via cette zone de saisie libre sont soumises aux dispositions applicables en matière de protection des données à caractère personnel, que vous vous engagez à respecter (données licites, objectives, pertinentes, adéquates et limitées à ce qui est nécessaire par rapport à la finalité poursuivie, loyauté de la collecte et du traitement des données, etc.). »*

- les écrans de la solution permettant la réalisation de reportings ou d'extractions incluent une mention d'avertissement à l'attention des utilisateurs de la solution, comme suit :

> *« En réalisant un export de ces données, vous devez vous assurez que vous agissez dans le respect des principes applicables en matière de protection des données à caractère personnel. Vous devez notamment vous assurer que le fichier qui va être créé sera utilisé uniquement dans le prolongement du traitement initial et en particulier, pour les mêmes finalités que celles poursuivies dans le cadre de la présente application. Vous devez également vous assurer que les données extraites sont pertinentes, adéquates et strictement nécessaires au regard de la finalité pour laquelle vous envisagez de les utiliser et ne les communiquer qu'aux personnes autorisées. Il vous incombe de veiller à prendre toutes les mesures destinées à en assurer la sécurité, et notamment la confidentialité. Le fichier export ne doit pas être conservé au-delà de la durée prévue pour les données traitées dans le cadre de la présente application ».*

4.4 Utilisation de cookies dans le cadre de l'interface ou du module web

4.4.1 Principes

SecuTix 360° permet l'analyse du comportement des internautes au moyen de la solution Google Analytics. Cette fonctionnalité de mesure d'audience et de statistiques de visites et de navigation peut être utilisée soit par votre organisme soit par SecuTix SA dans le but d'améliorer le service.

L'internaute doit être informé de l'utilisation des cookies de Google Analytics et consentir à leur dépôt et à leur exploitation.

Pour ce faire, l'internaute qui se rend sur le site web (page d'accueil ou page secondaire) doit être informé, par l'apparition d'un bandeau :

- des finalités précises des cookies utilisés ;
- de la possibilité de s'opposer à ces cookies et de changer les paramètres en cliquant sur un lien présent dans le bandeau (ce lien devant renvoyer à une

politique « cookies » présentant aux internautes de manière simple et intelligible des solutions mises à leur disposition pour accepter ou refuser tout ou partie des cookies) ;

- du fait que la poursuite de sa navigation vaut accord au dépôt de cookies sur son terminal.

Dans la mesure où le consentement ne doit pas être ambigu, ce bandeau ne doit pas disparaître tant que la personne n'a pas poursuivi sa navigation, c'est-à-dire tant qu'elle ne s'est pas rendue sur une autre page du site ou n'a pas cliqué sur un élément du site (image, lien, bouton « rechercher »).

Ainsi, sauf consentement préalable de l'internaute, le dépôt et la lecture de cookies soumis au consentement ne doivent pas être effectués :

- si l'internaute se rend sur le site et ne poursuit pas sa navigation : une simple absence d'action ne saurait être en effet assimilée à une manifestation de volonté ;
- s'il clique sur le lien présent dans le bandeau lui permettant de paramétrer les cookies et, le cas échéant, refuse le dépôt de cookies.

Enfin, les personnes ayant donné leur consentement au dépôt ou à la lecture des cookies doivent être en mesure de le retirer à tout moment. En cas de consentement de la personne concernée, celui-ci doit en tout état de cause être redemandé à l'issue d'un délai de 13 mois (cf. durée de vie maximum des cookies).

Pour information, il existe une dérogation à la nécessité de recueil du consentement pour les cookies de mesure d'audience si les conditions suivantes sont réunies :

- l'internaute est informé (cf. bandeau) ;
- il dispose de la faculté de s'y opposer par l'intermédiaire d'un mécanisme d'opposition facilement utilisable sur l'ensemble des terminaux, des systèmes d'exploitation, des applications et des navigateurs internet ; aucune information relative aux personnes ayant décidé d'exercer leur droit d'opposition ne doit être collectée et transmise à l'éditeur de l'outil d'analyse de fréquentation ;
- la finalité du dispositif doit être limitée à la mesure d'audience du contenu visualisé afin de permettre une évaluation des contenus publiés et de l'ergonomie du site ou de l'application ;
- les données collectées ne doivent pas être recoupées avec d'autres traitements (fichiers clients ou statistiques de fréquentation d'autres sites, par exemple) ; l'utilisation du cookie déposé doit être strictement cantonnée à la production de statistiques anonymes ; sa portée doit être limitée à un seul éditeur et ne doit pas permettre le suivi de la navigation de la personne utilisant différentes applications ou naviguant sur différents sites internet ;
- l'utilisation de l'adresse IP pour géolocaliser l'internaute ne doit pas fournir une information plus précise que la ville ; cette adresse IP doit également être supprimée ou anonymisée une fois la géolocalisation effectuée, pour éviter toute autre utilisation de cette donnée ou tout recoupement avec d'autres informations personnelles ;
- s'agissant des cookies, ils ne doivent pas avoir une durée de vie excédant treize mois et cette durée ne doit pas être prorogée automatiquement lors des

nouvelles visites ; les informations collectées par l'intermédiaire des cookies doivent être conservées pendant une durée de treize mois maximum.

4.4.2 La solution SecuTix 360°

En votre qualité d'éditeur du site internet (que vous utilisiez notre interface web ou notre module web intégré dans votre propre site internet), il vous appartient d'informer et de recueillir le consentement des internautes en vue du dépôt et de la lecture des cookies.

A cet égard, nous vous informons que :

- sur demande auprès de notre service en charge du support, notre interface et notre module web vous proposent l'affichage d'un bandeau d'information et de recueil du consentement à l'installation de cookies lors de la première visite d'un internaute. La formulation de l'information à communiquer aux internautes via ce bandeau est de votre responsabilité. A toutes fins utiles, nous vous proposons la formulation suivante, à charge pour vous de la modifier ou de l'ajuster en fonction des spécificités éventuellement liées à votre propre site internet :

> En continuant votre navigation sur ce site, vous acceptez l'utilisation de cookies ou technologies similaires ayant pour finalité la réalisation de statistiques de visites sur notre site (tests et mesures d'audience, de fréquentation, de navigation, de performance), mais également *[à compléter le cas échéant avec d'autres finalités en fonction de votre interface web]*.
> Pour en savoir plus et paramétrer vos choix en matière de cookies et autres technologies similaires, cliquer ici *[insérer un lien vers la politique cookies]*.

Un tel bandeau doit être implémenté que vous utilisiez notre interface web ou notre module web intégré dans votre site internet. Ce bandeau doit être implémenté sur la 1ère page du site sur laquelle se rend l'internaute, même s'il s'agit d'une page secondaire et non de la page d'accueil ;

- La rédaction de la « politique cookies » est de votre responsabilité. Toutefois, nous vous informons que les cookies que nous utilisons dans le cadre de votre interface web sont les suivants :

Type	Nom	Editeur	Finalités	Durée
Cookie permanent de statistique et de suivi de mesure d'audience et de fréquentation	_ga	Google Inc. (Google Analytics)	Si google Analytics est activé, ces cookies sont mis en œuvre sur la base d'informations recueillies lors de la navigation de l'utilisateur, notamment l'adresse url depuis laquelle l'utilisateur a accédé au site, le fournisseur d'accès à internet de l'utilisateur, le type, la configuration et le paramétrage du navigateur,… Ces cookies sont utilisés pour distinguer les visiteurs uniques sur un site en attribuant un numéro généré de façon aléatoire comme un identifiant utilisateur. Ce dernier est mis à jour	En fonction des choix de paramétrage du client

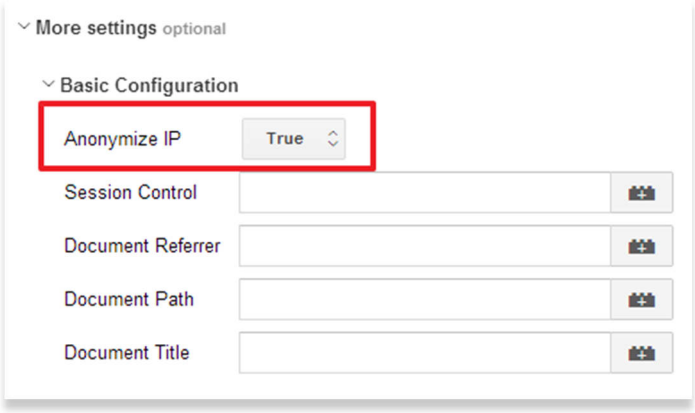
			à chaque page vue et permet notamment de calculer le nombre de visiteurs, de sessions,… Pour en savoir plus : https://support.google.com/analytics/answer/6004245 Module de désactivation de Google Analytics : https://support.google.com/analytics/answer/181881?hl=fr&ref_topic=2919631. ou https://tools.google.com/dlpage/gaoptout.	
Cookie limité à la session	lang		Ce cookie permet de se souvenir du choix de langue du contact.	Session
Cookie de session à but technique	SESSION		Identifiant technique de la session.	Session
Cookie limité à la session à but technique	BIGipServer_XXX		Ce cookie permet de router le contact vers la même machine afin de bénéficier d'options de caching.	Session
Cookie limité à la session à but technique	AcpAT_XXX		Ce cookie permet de valider que le contact est bien passé par PeakProtect (outil de gestion des fortes affluences)	Session

Ces éléments d'information devront être insérés par vos soins dans votre politique cookies.

Une telle politique cookie doit être implémentée que vous utilisiez notre interface web ou notre module web intégré dans votre site internet ;

- par principe, il convient que les cookies ne s'installent pas tant que l'internaute n'a pas continué sa navigation et le bandeau doit réapparaître à l'issue d'un délai de 13 mois à compter de l'obtention du consentement aux cookies. C'est cette configuration qui est proposée par défaut sur les interfaces web mises à disposition par SecuTix SA suite à une demande de service votre part en ce sens. Il convient que vous vous assuriez du respect de cette obligation sur votre propre site internet également si vous utilisez notre module intégré dans votre site internet ;

- si vous souhaitez vous soustraire à cette obligation de consentement (afin que les cookies puissent s'installer dès la page d'accueil), il convient de paramétrer les cookies selon les principes rappelés supra concernant les cookies de mesure d'audience non soumis au consentement. Notamment (mais non exclusivement), il convient qu'un opérateur de votre organisme configure Google Analytics pour rendre anonyme des adresses IP avant l'envoi des données chez Google aux Etats-Unis afin qu'aucun recoupement personnel ne soit possible :



Les autres obligations nécessaires à cette exception au consentement devront également être respectées.

Attention, cette exception au consentement n'est valable que pour les cookies de mesure d'audience : l'utilisation de cookies autre tels que les cookies de réseaux sociaux ou encore les cookies publicitaires demeurent soumis à un consentement préalable de l'internaute.

4.5 Durée de conservation des données

4.5.1 Principes

Les dispositions en matière de protection des données à caractère personnel imposent au responsable de traitement de ne conserver les données que pour une durée proportionnée aux finalités poursuivies. En revanche, elles ne donnent pas d'indications sur la durée exacte de conservation. Le stockage illimité des données personnelles n'est en tout état de cause pas autorisé.

4.5.2 La solution SecuTix 360°

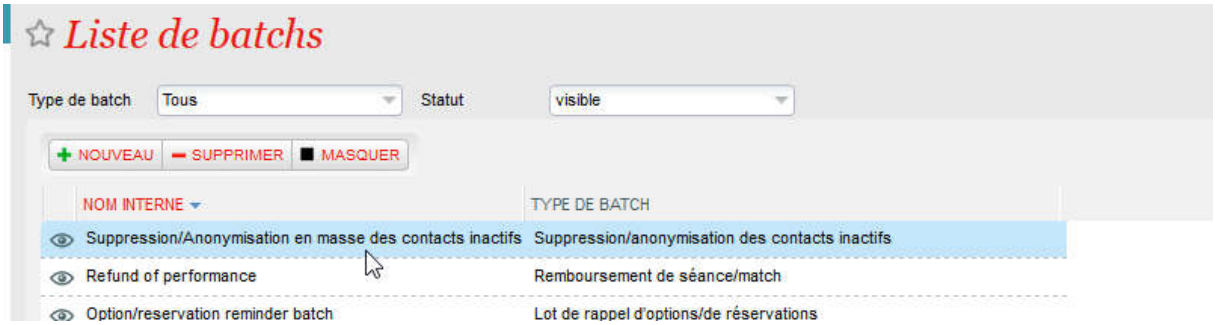
En votre qualité de responsable de traitement, il vous appartient de déterminer et de faire appliquer une durée maximum de conservation des données dans les outils que vous utilisez pour le traitement de données à caractère personnel, et notamment dans la solution SecuTix 360°. Cette durée de conservation maximum concerne les données de l'ensemble des personnes concernées dont les données sont collectées et traitées dans la solution SecuTix 360°.

La solution SecuTix 360° proposent plusieurs fonctionnalités en vue de la suppression des données par vos soins :

- les contacts disposant d'un compte personnel en ligne ont la possibilité de supprimer leurs données depuis ce compte :

- les opérateurs de votre organisme ont la possibilité de supprimer des contacts :

- dans ces deux cas, le compte du contact est supprimé, les informations de marketing (historique et indicateurs) sont supprimées et toutes les commandes sont rendues anonymes. L'anonymisation des données devient irréversible lors de la suppression des logs, c'est-à-dire à l'issue d'un délai de 12 mois (cf. durée de conservation des logs) ;
- les opérateurs de votre organisme ont la possibilité de supprimer les prospects ;
- les opérateurs de votre organisme ont la possibilité d'anonymiser manuellement les données de toute personne concernée ;
- SecuTix 360° comporte aussi une fonctionnalité, mise à votre disposition, vous permettant selon vos choix, vos pratiques, votre secteur d'activité et les dispositions qui vous sont applicables, de détecter les contacts inactifs depuis plus que X mois et les supprimer/anonymiser en masse :



- après avoir mis un compte opérateur à l'état « suspendu », vous pouvez l'anonymiser simplement en remplaçant son nom/prénom/email/etc. par XXXX. L'anonymisation des données devient irréversible lors de la suppression des logs, c'est-à-dire à l'issue d'un délai de 12 mois (cf. durée de conservation des logs). Attention, il est impossible de modifier / anonymiser le code de connexion des opérateurs. Aussi,il est de la responsabilité des administrateurs créant les opérateurs de ne pas y mettre une information permettant d'identifier l'individu.

En tout état de cause, à l'issue du contrat, vos données sont extraites et vous sont restituées dans un format standard au regard de l'état de l'art et du marché. Elles sont ensuite supprimées de la solution et suivent les mêmes règles de purges que lors d'une suppression manuelle (cf. ci-dessus).

4.6 Données exactes et à jour. Droits d'accès, de rectification, d'effacement et de portabilité. Droit à la limitation du traitement et droit d'opposition au traitement.

4.6.1 Principes

Aux termes des dispositions applicables en matière de protection des données à caractère personnel, les données traitées doivent être exactes, et, si nécessaire, tenues à jour. Des mesures appropriées doivent être prises par le responsable de traitement pour que les données inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées.

Les personnes concernées doivent se voir garantir un droit d'accès à leurs données, un droit à la portabilité de leurs données et un droit de rectification et d'effacement desdites données.

Par ailleurs, ces personnes bénéficient d'un droit à la limitation du traitement ainsi que d'un droit d'opposition au traitement de leurs données.

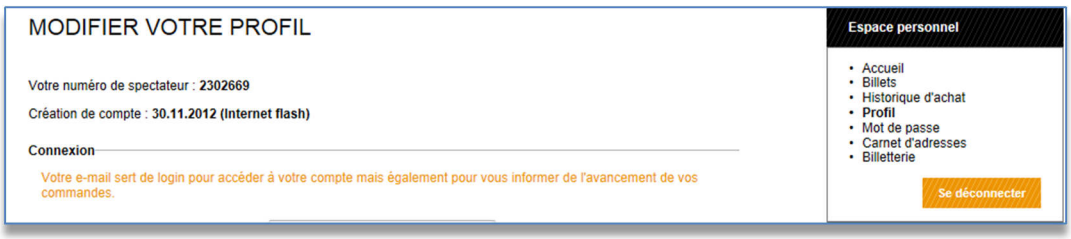
Ces obligations sont à la charge du responsable de traitement. Toutefois, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits précités.

4.6.2 La solution SecuTix 360°

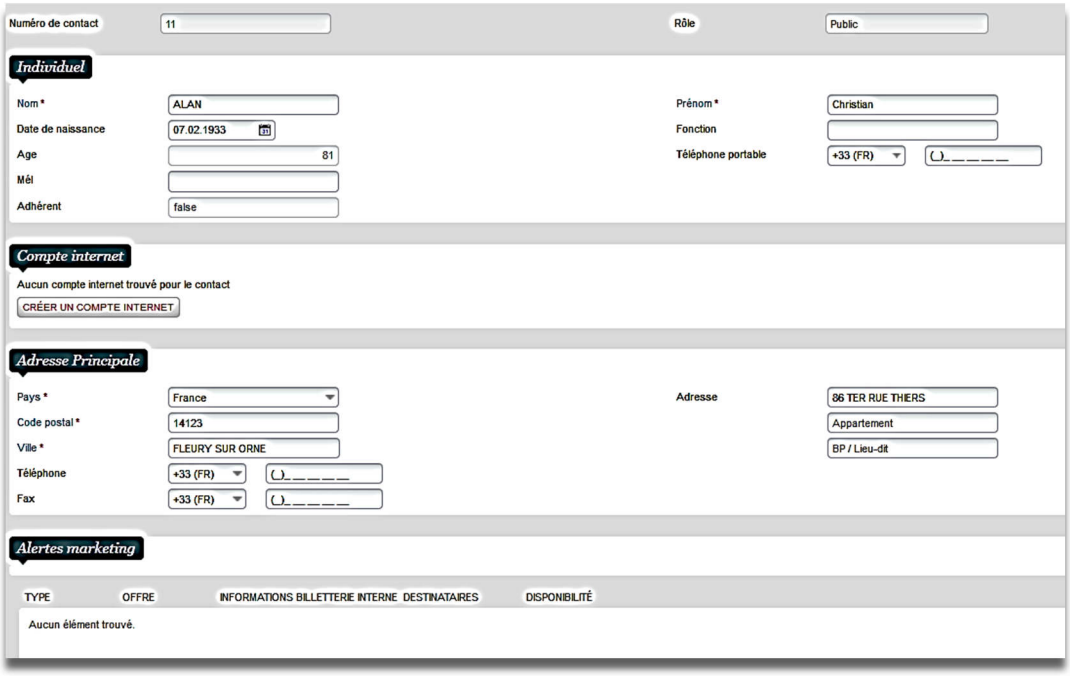
En qualité de responsable de traitement, vous devez vous assurer d'apporter aux personnes concernées les réponses prévues par les dispositions applicables en cas d'exercice par ces dernières de leurs droits précités, et que leurs demandes (sous réserve qu'elles remplissent les conditions requises) soient suivies d'effet. A cet égard, il est précisé qu'en cas de demande qui nous serait adressée directement, nous vous en informerons, la réponse à ces demandes et les actions devant être déployées en résultant demeurant de votre seule responsabilité.

SecuTix 360° dispose des fonctionnalités permettant la gestion des demandes de rectification ou d'effacement de données présentes au sein de la base de données de SecuTix 360°.

- les internautes peuvent à tout moment modifier les données de leur profil dans leur compte personnel en ligne :



- les opérateurs de votre organisme peuvent mettre à jour les fiches contacts :



- concernant les demandes d'effacement des données, voir le paragraphe 4.5.

Un contact peut demander l'ensemble des informations personnelles le concernant dans le cadre de l'exercice de son droit d'accès ou de son droit à la portabilité de ses données. Les opérateurs de votre organisme ont accès aux données des contacts pour répondre à ces demandes. Par ailleurs, sur demande auprès de SecuTix SA, un opérateur de votre organisme peut obtenir l'ensemble des informations stockées concernant un contact (fiche contact, historique d'achat, historique relationnel).

En outre :

- l'origine des informations de la fiche contact est indiquée sous la forme « information saisie par l'internaute », « information saisie par un opérateur de votre organisme », « information collectée par import de données » :

- la date de création d'un compte personnel est disponible dans ledit compte :

- la date de création d'une fiche contact et la date de la dernière modification sont indiquées dans la fiche contact :

Enfin, il vous appartient de gérer dans la solution les demandes de limitation du traitement ou d'opposition au traitement des données.

En tout état de cause, nous nous engageons à mettre en œuvre tous les moyens pour vous communiquer, sur demande, les éléments en notre possession permettant d'apporter une réponse aux demandes d'exercice de leurs droits par les personnes concernées.

4.7 Sécurité des données

4.7.1 Principes

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Des mesures de sécurité et de confidentialité adéquates doivent donc être mises en œuvre. Pour des recommandations en matière de sécurité des données, vous pouvez vous reporter à : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles.

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Par ailleurs, en cas de violation de données à caractère personnel (à savoir, toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement), le responsable du traitement se voit mettre à sa charge une obligation de notification auprès de l'autorité de contrôle compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

4.7.2 La solution SecuTix 360°

En votre qualité de responsable de traitement, il vous appartient de vous assurer du respect de l'ensemble de ces obligations.

SecuTix SA, en sa qualité de sous-traitant, se voit mettre à sa charge une obligation de déploiement des mesures de sécurité appropriées, de notification au responsable du traitement de toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance, et plus généralement une obligation de coopérer avec le responsable de traitement en vue du respect par ce dernier de ses propres obligations (déploiement des mesures appropriées de sécurité et analyse d'impact notamment).

SecuTix SA garantit satisfaire les exigences et avoir obtenu les certificats de conformité aux normes ISO/IEC 27001:2013 et PCI DSS v3.2. Ainsi, SecuTix SA s'engage à mettre en œuvre les mesures techniques et organisationnelles de sécurité identifiées dans ces normes.

Par ailleurs, s'agissant de la solution SecuTix 360° :

- Les données sont dupliquées en temps réel sur plusieurs disques redondants.
- Les données sont dupliquées en quasi temps réel dans deux Datacenters distants de plusieurs kilomètres.
- Pour sécuriser les serveurs et la solution de manière appropriée, SecuTix SA prend toutes les mesures techniques et organisationnelles nécessaires, notamment les contrôles d'accès, l'utilisation de pare-feu et programmes anti-

virus actuels, des cryptages SSL et des journaux/logs lors des changements manuels des banques de données.

- La partie monétaire de SecuTix 360° est certifiée PCI DSS et auditée une fois par année.
- Les mots de passe doivent avoir un nombre et une combinaison sûre de caractères et de chiffres pour être valides.
- SecuTix 360° possède un plan de continuité pour le passage d'un Datacenter à l'autre.
- Les accès physiques des personnes dans les Datacenters sont strictement contrôlés par code, traçage, alarmes, badges, vidéosurveillance.
- Les données envoyées au site de secours sont chiffrées via VPN ou HTTPS.

En outre, conformément à nos obligations, nous nous engageons à coopérer avec vous en vue :

- du respect par vos soins de vos propres obligations en matière de sécurité et notamment de confidentialité des données à caractère personnel ;
- de la réalisation par vos soins des analyses d'impact des traitements sur la protection des données à caractère personnel si la nature des traitements dans le cadre desquels nous intervenons l'exige, et de l'éventuelle consultation de l'autorité de contrôle le cas échéant s'agissant de ces mêmes traitements de données.
- du respect de votre obligation de notification à l'autorité de contrôle et d'information de la personne concernée en cas de violation de données à caractère personnel. A cette fin, nous vous notifierons toute violation de données à caractère personnel dont nous aurions eu connaissance. Nous nous engageons également à mettre en œuvre tous les moyens et à vous communiquer, à votre demande, la documentation en notre possession qui serait utile afin de vous permettre, si nécessaire, de procéder aux notifications précitées lorsqu'elles sont requises.

Il convient également que vous preniez les mesures techniques et organisationnelles opportunes au sein de votre organisme pour contribuer à l'atteinte d'un niveau approprié de sécurité des données traitées dans le cadre de la solution SecuTix 360°. Aussi, il est recommandé, par exemple, de :

- protéger et maintenir les accès à SecuTix 360° actuels (Hardware, software, Réseau, Accès Internet) ;
- assurer la confidentialité des mots de passe avec lesquels les opérateurs de votre organisme se connectent à SecuTix 360° et veiller à ce qu'une politique de mot de passe soit déployée conformément aux recommandations applicables (cf. voir à titre d'illustration les recommandations accessibles ici : https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires) ;
- tenir à jour l'antivirus sur tous les postes de travail ;
- …

4.8 Sous-traitants, sous-traitants ultérieurs et flux transfrontières

4.8.1 Principes

Le recours à des sous-traitants et à des sous-traitants ultérieurs pour le traitement des données à caractère personnel doit faire l'objet d'un encadrement contractuel spécifique comportant un certain nombre de clauses obligatoires.

Les flux transfrontières de données vers des Etats non membres de l'UE et non reconnus comme assurant un niveau de protection adéquate des données peuvent être mis en œuvre sous réserve de garanties suffisantes, notamment contractuelles.

4.8.2 La solution SecuTix 360°

Dans le cadre de la mise à disposition de la solution SecuTix 360° à l'attention de votre organisme, nous pouvons être amenés à traiter des données à caractère personnel pour votre compte en qualité de sous-traitant. Les documents contractuels que nous vous proposons comportent une clause conforme aux exigences du RGPD visant à encadrer nos prestations en cette qualité de sous-traitant pour votre compte en matière de traitements de données à caractère personnel.

En vue de la fourniture de cette solution, les différentes entités de notre groupe peuvent également être amenées à traiter des données à caractère personnel pour votre compte. A cet égard, nous vous informons que les entités de notre groupe sont principalement établies en Union européenne ou en Suisse, pays assurant un niveau adéquat de protection des données. Toutefois, une entité est établie au Vietnam. Conformément aux dispositions applicables en matière de protection des données, les flux transfrontières de données vers cette entité sont encadrés par une convention de flux transfrontières élaborée sur la base des modèles suisses proposés par le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT) et des modèles européens établis par la Commission européenne.

Par ailleurs, pour vous fournir l'ensemble des fonctionnalités proposées dans le cadre de la solution SecuTix 360°, nous pouvons être amenés, en fonction des prestations et services que vous avez souscrits, à avoir recours à des sous-traitants ultérieurs dont vous trouverez la liste en Annexe 2.

4.9 Utilisation des données à des fins marketing

4.9.1 Principes

S'agissant de l'utilisation des données à des fins de marketing, les principes suivants sont applicables :

- nécessité d'un consentement exprès (opt-in au moyen d'une case à cocher non pré-cochée rédigée de manière positive) pour les échanges par courrier électronique, sms, mms, télécopie et système automatisé de communications électroniques (cf. automate d'appels par exemple) ;
- nécessité d'une absence d'opposition préalable pour les échanges par courrier électronique ou téléphonie avec intervention humaine ;
- chaque envoi (notamment email et sms) doit comprendre un moyen simple et gratuit de désinscription (droit d'opposition) aux communications par cette voie +

nécessité pour les envois par voie électronique d'indiquer un objet en lien avec le contenu et de préciser pour le compte de quel annonceur elle est adressée.

Pour ce qui concerne les envois par courrier électronique, sms ou mms, il convient de préciser qu'une exception au consentement peut être invoquée sous réserve que les conditions cumulatives suivantes soient remplies :

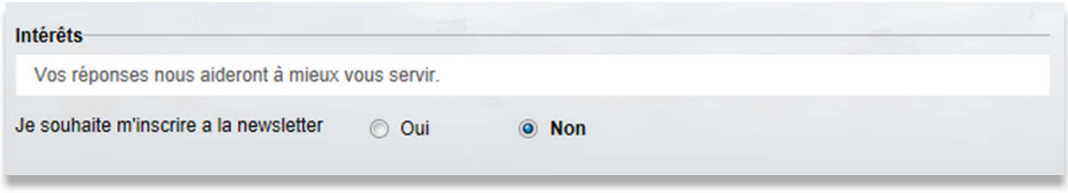
- les coordonnées du destinataire ont été recueillies auprès de lui à l'occasion d'une vente ou d'une prestation de services ;
- dans le respect des dispositions applicables en matière de protection des données à caractère personnel, notamment s'agissant de l'information des personnes ;
- la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale ;
- le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées au moment où elles sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé.

4.9.2 La solution SecuTix 360°

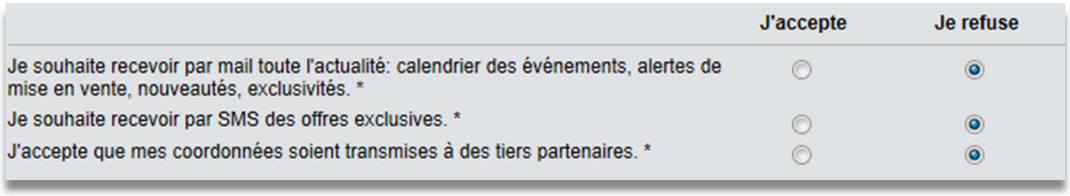
SecuTix 360° vous propose des fonctionnalités de marketing permettant d'adresser des messages publicitaires à vos contacts (clients et prospects). Vous demeurez néanmoins seul responsable de l'utilisation que vous faites de ces fonctionnalités, et devez respecter les principes susvisés.

Pour vous permettre de réaliser vos opérations marketing conformément aux principes précités, SecuTix SA a mis en place les fonctionnalités suivantes :

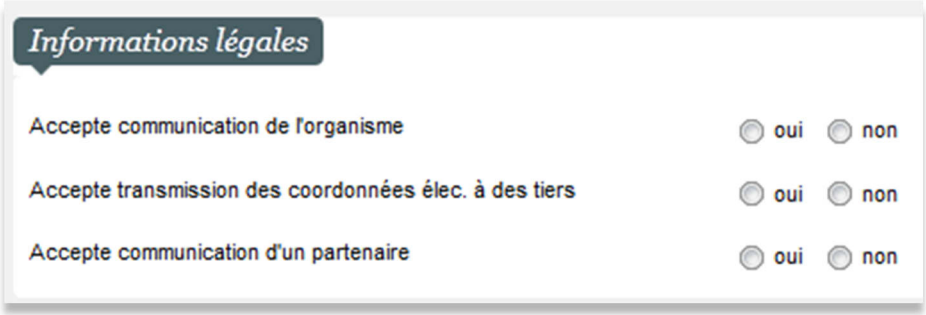
- le formulaire de création de compte personnel en ligne par un internaute via notre interface ou notre module web comporte un encart destiné à y intégrer la mention d'information dont la rédaction vous appartient. Cette mention devra être complétée par vos soins avec les cases à cocher (non pré-cochée) et les phrases de recueil de consentement / opposition imposées. Ces éléments se paramètrent dans le « point de vente » internet ;
- les internautes disposent par défaut de plusieurs fonctionnalités dans leur compte personnel en ligne, comme suit :
  - inscription / désinscription à la/les newsletters (adaptable à vos besoins) :



- choix de réception des médias de communication et des expéditeurs (adaptable à vos besoins):



- au guichet (dans le back-office) :
  - un opérateur de votre organisme peut déterminer si un contact accepte de recevoir des communications de votre organisme, de partenaires de votre organisme ou de tiers :



- un opérateur peut déterminer les canaux de communication désirés par le contact :

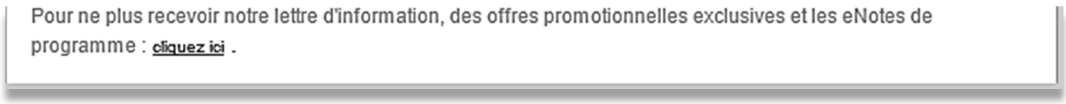
- par défaut, aucun choix n'est coché. Aussi tout « cochage » résulte nécessairement d'une action positive de l'internaute ou d'un opérateur. Il convient que vous teniez compte de ces règles de gestion en vue de la réalisation de vos opérations de marketing conformément aux principes visés au paragraphe 4.9.1.

  Par ailleurs, il convient que vous teniez compte des demandes d'opposition à la prospection portées à votre connaissance par les personnes concernées, en fonction des médias visés (en cochant les moyens de communication visés à « non »).

Aux fins de sensibilisation des utilisateurs de la solution, SecuTix 360° intègre une mention d'avertissement à leur attention sur les écrans permettant la réalisation d'opérations de prospection, rédigée comme suit :

> *« Dans le cadre des opérations de prospection que vous souhaitez déployer, nous vous rappelons qu'il convient que vous teniez compte des principes suivants :*
>
> - *il est interdit de prospecter un contact via un moyen de communication coché à « non » ;*
> - *la prospection par email, sms, mms, télécopie ou encore système automatisé de communications électroniques est possible uniquement via un moyen de communication coché à « oui » ;*
> - *la prospection par courrier postal ou par télémarketing est possible via un moyen de communication coché à « oui » ou non coché (cf. ni « oui » ni « non »). »*

Les newsletters envoyées par SecuTix 360° à votre demande comportent, a minima, les informations permettant aux destinataires d'exercer leur droit d'opposition (i.e. leur volonté de ne plus recevoir de tels envois). En effet, dans ces communications, un lien permet de se désabonner. Le désabonnement est pris en considération automatiquement dans SecuTix 360° (cochage mis à « non ») :



Pour inclure cette fonctionnalité dans vos envois par emails, veuillez inclure dans la configuration des emails envoyés l'une des deux solutions ci-dessous :

- dans l'email envoyé, l'opérateur de votre organisme configure le lien « Unsubscribe URL ». Le désabonnement a lieu automatiquement lorsque le contact clique sur le lien :

- dans l'email envoyé, l'opérateur de votre organisme met un lien qui redirige vers l'espace personnel. Le contact va pouvoir décocher son abonnement ou modifier ses préférences dans son espace personnel.

4.10 Formalités

4.10.1 Principes

Chaque responsable du traitement tient un registre des activités de traitement effectuées sous sa responsabilité.

Chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte de responsables du traitement.

Ces registres doivent se présenter sous une forme écrite y compris électronique. Le responsable du traitement ou le sous-traitant mettent le registre à la disposition de l'autorité de contrôle sur demande.

4.10.2 La solution SecuTix 360°

En qualité de responsable de traitement, vous devez intégrer les traitements de données à caractère personnel mis en œuvre au moyen de la solution SecuTix 360° dans votre registre « responsable de traitement » des activités de traitements.

De notre côté, en qualité de sous-traitant, nous intégrons les traitements de données à caractère personnel mis en œuvre au moyen de la solution SecuTix 360° pour votre compte dans notre registre « sous-traitant » des activités de traitements.

Annexe 1. Check-list à compléter par votre organisme concernant les traitements de données à caractère personnel mis en œuvre dans la solution SecuTix 360°

Question	Réponse
Finalités d'utilisation de la solution et prestations / services souscrits	
Données collectées et traitées dans la solution	…
Personnes autorisées à ajouter de nouveaux champs + modalité des demandes en ce sens auprès de SecuTix SA	
Personnes autorisées à ajouter de nouveaux critères de segmentation + modalité des demandes en ce sens auprès de SecuTix SA	
Personnes autorisées à ajouter de nouveaux critères de reportings / extractions + modalité des demandes en ce sens auprès de SecuTix SA	
Personnes habilitées à accéder aux données dans la solution	
Personnes autorisées à réaliser des reportings / extractions dans la solution	
Durée de conservation des données souhaitée dans la solution	
Contact au sein de l'organisme pour les demandes d'exercice de leurs droits par les personnes concernées	
Contact au sein de l'organisme en cas de violation de données	

Annexe 2. Liste des sous-traitants ultérieurs de SecuTix SA

Nom	Activité	Pays	Données à caractère personnel transférées
Amazon Web Services	Hébergement de fichiers publics	USA	No
Google Maps for Work	Normalisation, validation et auto-suggestion d'adresses postales	USA	No
Pca Predict	Normalisation, validation et auto-suggestion d'adresses postales	UK	No
Ingenico ePayment	Prestataire de service de paiement	France / Belgique	Yes
Datatrans	Prestataire de service de paiement	Suisse	Yes
Orange Business Services – Contact Everyone	Routage de SMS	France	Yes
Maxmind	Géolocalisation d'adresses IP	USA	Yes
EFSTA	Reçus fiscaux	Autriche	Yes
Nazaries	customer support	Espagne	Yes
SecuTix SA	Distributeur, support client	France	Yes
SecuTix Iberia S.L.	Distributeur	Espagne	Yes
SecuTix Ltd	Distributeur	UK	Yes
Elca Informatique SA	Software development, new customer onboarding, customer support, exploitation et maintenance, hébergement	Suisse	Yes
Elca Spain	Software development and integration, customer support	Espagne	Yes
Elca Information Technology Ltd	Software development, new customer onboarding, customer support, exploitation et maintenance	Vietnam	Yes
Eric David	Softw.dev, support, onboarding	Suisse	Yes
Agorasophia Edutainment Spa Management	sales and onboarding	Italie	Yes
Swantegy USA LLC	sales and onboarding	USA	Yes
Softjourn, Inc	Sales and onboarding	USA	No