

S-360 Guide de protection des données

Date	9 th février 2024
Auteur	CPF
Réviseur	OSR / FABJ
Version	2.8

Table des matières

1	Introduction	2
2	Définitions	3
3	Exigences réglementaires	3
4	Caractéristiques de S-360	5
4.1	Finalités légitimes et légalité du traitement des données	5
4.2	Équité et transparence dans la collecte et le traitement des données	6
4.3	La pertinence, l'adéquation et la stricte nécessité des données	9
4.4	Utilisation de cookies dans l'interface web ou le module	14
4.5	Période de conservation des données.....	17
4.6	Des données exactes et à jour. Droits d'accès, de rectification, d'effacement et de portabilité. Droits de restriction du traitement et d'opposition.....	19
4.7	Sécurité des données.....	21
4.8	Sous-traitants des données et transferts transfrontaliers	24
4.9	Utilisation des données à des fins de marketing	25
4.10	Formalités	28
	Annexe 1 Liste de contrôle à remplir par votre organisation concernant le traitement des données à caractère personnel effectué à l'aide de S-360	30
	Annexe 2 Liste des sous-traitants de SECUTIX SA	32
	Annexe 3 Durée de conservation des documents	33

1 Introduction

Dès lors que votre organisation utilise la plateforme S-360 fournie par SECUTIX SA, celle-ci agit en tant que responsable du traitement des données en ce qu'elle collecte et traite des données personnelles concernant notamment les clients qui achètent des billets, les prospects, vos propres opérateurs, etc. De même, SECUTIX SA peut agir en tant que sous-traitant en transférant et/ou traitant ces données pour fournir la solution ainsi que les services auxquels votre organisation souscrit.

Lors de la collecte, du traitement et du transfert de ces données personnelles, vous devez vous conformer aux réglementations applicables en matière de protection des données. En tant que responsable du traitement des données, vous êtes seul responsable du respect des exigences en matière de protection des données qui s'appliquent à vous.

Dans l'Union européenne, la réglementation applicable est issue du 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. Ce texte est connu sous le nom de règlement général sur la protection des données (RGPD). Il est directement applicable dans tous les États membres de l'Union européenne depuis le 25 mai 2018.

SECUTIX SA est soumise à la législation suisse sur la protection des données (voir encadré ci-dessous). Cette législation est très similaire (identique dans certains cas) à la réglementation de l'UE. La Commission européenne a également décidé (décision de la Commission 2000/518 CE du 15.01.2024) que la Suisse assure une protection adéquate des données personnelles transférées depuis l'UE.

En outre, SECUTIX SA veillera à ce que la solution qu'elle vous fournit vous permette de vous conformer aux exigences de protection des données applicables en la matière. Ce document, non exhaustif, présente les options techniques et organisationnelles pertinentes incluses dans S-360.

Préliminaires

Tout d'abord, nous déclarons que :

- Ce guide sur la protection des données a pour seul but de vous faire connaître les caractéristiques pertinentes de S-360 et les précautions que nous avons prises pour vous aider à vous conformer à certaines exigences légales ou réglementaires qui peuvent s'appliquer à vous en tant que responsable du traitement des données.
- Ce document ne constitue pas un ensemble d'instructions à suivre, ni un avis juridique.
- Les finalités pour lesquelles vous traitez les données et les moyens que vous utilisez pour ce faire relèvent de votre seule décision et de votre seule responsabilité. Par conséquent, vous devez nous transmettre vos instructions en utilisant la liste de contrôle figurant à l'annexe 1.

2 Définitions

Données à caractère personnel : Toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée 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 l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique (ci-après dénommées "données à caractère personnel").

Traitement : Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou à 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 divulgation 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 du traitement des données : 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 des données à caractère personnel. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou des États membres, le responsable du traitement (désigné dans le présent document par "vous" ou "votre organisation") ou les critères spécifiques de sa nomination peuvent être prévus par le droit de l'Union ou des États membres.

Sous-traitant des données : Une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite les données personnelles pour le compte du contrôleur de données (désigné dans le présent document par "nous" ou "SECUTIX SA").

Personne concernée : Personne physique dont les données à caractère personnel font l'objet d'un traitement dans le cadre de S- 360.

Violation de données à caractère personnel : Une violation de la sécurité entraînant accidentellement ou illégalement la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, stockées ou traitées d'une autre manière, ou l'accès à ces données.

3 Exigences réglementaires

Les lois sur la protection des données exigent que tous les contrôleurs de données respectent les principes suivants :

- Les données sont collectées et traitées de manière licite, loyale et transparente.
- Les données sont traitées pour des finalités déterminées, explicites et légitimes. Les données à caractère personnel ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.
- Les données collectées et traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Elles sont exactes et mises à jour. Certaines données à caractère sensible ne sont

collectées et traitées que sous certaines conditions, notamment avec le consentement de la personne concernée.

- Les données sont conservées pendant une durée n'excédant pas celle strictement nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.
- Les personnes concernées sont informées que leurs données à caractère personnel seront traitées et leur consentement est demandé pour certains types de traitement. Certaines informations qui doivent être fournies à ces personnes sont obligatoires.
- Les personnes concernées ont un droit garanti d'accès et de rectification ou d'effacement des données à caractère personnel, ainsi que le droit de restreindre le traitement ou de s'y opposer, et le droit à la portabilité des données. Les personnes concernées ont également le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques à leur égard ou qui les affecte de manière significative de façon similaire.
- Les responsables du traitement prennent les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données, en particulier pour empêcher la destruction accidentelle ou illicite, la perte, l'altération ou la divulgation non autorisée de données. (Dans certains cas, une analyse d'impact sera nécessaire pour déterminer si les mesures prévues sont adéquates. Cela peut nécessiter que le responsable du traitement des données consulte l'autorité de contrôle compétente). Les violations de données à caractère personnel doivent également être signalées à l'autorité de contrôle par le biais d'une procédure de notification spécifique et, dans certains cas, aux personnes concernées.
- Les responsables du traitement qui font appel à des sous-traitants et sous-traitants ultérieurs pour traiter des données à caractère personnel doivent le faire dans un cadre contractuel spécifique (cf. clauses obligatoires).
- Les flux transfrontaliers de données à caractère personnel vers des États non-membres de l'UE qui ne sont pas reconnus comme offrant un niveau de protection adéquat doivent être soumis à des garanties suffisantes et, en particulier, contractuelles.
- Toute organisation qui recueille et traite des données à caractère personnel doit établir et conserver :
 - les registres des activités de traitement des données à caractère personnel mises en œuvre sous sa responsabilité en tant que contrôleur des données
 - des registres des activités de traitement des données à caractère personnel mises en œuvre sous sa responsabilité en tant que responsable du traitement des données.

Focus - principes et engagements en matière de protection des données en Suisse (loi fédérale sur la protection des données) :

Tout traitement de données doit être licite :

- Tout traitement doit être conforme aux principes de bonne foi et de proportionnalité. Les données à caractère personnel ne sont traitées qu'aux fins indiquées lors de la collecte, ou aux fins prévues par la loi ou par les circonstances.
- Les personnes concernées doivent être informées de la collecte de leurs données à caractère personnel et, en particulier, des finalités pour lesquelles ces données seront utilisées.
- Lorsque leur consentement est requis pour le traitement de leurs données à caractère personnel, ce consentement n'est valable que s'ils le donnent librement et après avoir été dûment informés.

- En outre, leur consentement au traitement des données sensibles et des profils de personnalité doit être explicite. Les données à caractère personnel sont protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées.

4 Caractéristiques de S-360

Ce paragraphe (4) décrit :

- les exigences et obligations auxquelles vous devez vous conformer conformément au paragraphe 3 ci-dessus
- les caractéristiques et propriétés de S-360 qui vous permettent de le faire.

4.1 Finalités légitimes et légalité du traitement des données

4.1.1 Principes

Le contrôleur des données est chargé de veiller à ce que

- les données sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités (cf. principe de finalité)
- les données sont collectées et traitées légalement dans le cadre de S-360 (cf. principe de légalité).

Il convient de noter que le traitement n'est licite que si et dans la mesure où au moins l'une des conditions suivantes s'applique :

- La personne concernée a donné son consentement 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 pour prendre des mesures à la demande de la personne concernée avant de conclure un contrat.
- Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.
- Le traitement est nécessaire pour protéger les 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 à 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, sauf lorsque ces intérêts sont supplantés par les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, en particulier lorsque la personne concernée est un enfant.

4.1.2 S-360

La solution informatique S-360 comprend les caractéristiques suivantes :

- Gestion de la billetterie : configuration, planification, réservation, vente, émission, impression, contrôle d'accès, gestion des opérateurs, etc.
- Gestion de la relation client (clients et prospects) : campagnes de marketing, activités de prospection et de sollicitation et opérations associées : sélection, segmentation, enrichissement des données, ciblage, courrier électronique, analyse et suivi (navigation sur le site web et courriers électroniques) et rapports (statistiques et performances).
- Gestion d'événements : organisation, planification, conférenciers/guides, etc.
- Gestion des ventes en ligne et sur site : gestion des stocks, des approvisionnements et des fournisseurs.

En tant que responsable du traitement des données, vous avez choisi S-360 comme le système le plus approprié pour traiter les données à caractère personnel à des fins que vous avez déterminées et qui sont spécifiques à vos activités. Il vous incombe de veiller au respect des principes de finalité et de licéité énoncés ci-dessus.

4.2 Équité et transparence dans la collecte et le traitement des données

4.2.1 Principes

Les responsables du traitement informent les personnes concernées de la manière dont leurs données à caractère personnel seront traitées (cf. principe de loyauté et de transparence) conformément aux dispositions applicables en matière de protection des données à caractère personnel. Dans certains cas, elles doivent également avoir donné leur consentement (cf. paragraphes 3.1, 4.3 et 4.9 en particulier).

En outre, tous les formulaires de collecte de données doivent contenir les informations pertinentes.

4.2.2 S-360 et clients finaux

Par conséquent, en tant que responsable du traitement des données, il vous incombe d'informer les personnes concernées comme indiqué ci-dessus et d'obtenir leur consentement le cas échéant. Naturellement, nous sommes heureux de vous fournir, sur demande, toute information que nous détenons et qui pourrait vous aider à le faire.

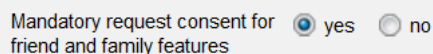
En outre, pour vous permettre de remplir vos obligations, nous vous informons des éléments suivants :

- L'interface web de S-360 comporte un onglet "Déclaration de confidentialité" (« Privacy Policy ») intégré. Il est accessible à partir de chaque page web et

comporte un lien hypertexte qui redirige les utilisateurs vers une page où vous pouvez ajouter votre propre déclaration ou politique de protection des données, qu'il vous incombe de rédiger :

© 2022 SECUTIX | CREATED BY SECUTIX | SITE MAP | GENERAL TERMS & CONDITIONS | PRIVACY POLICY | CONTACT US

- Si vous utilisez notre module web intégré dans votre site web, vous devez ajouter un onglet comme celui-ci à votre site.
- Tous les formulaires de collecte de données en ligne dans notre interface web et notre module web (s'il est intégré à votre site web) comprennent un encart (que vous êtes chargé de rédiger et d'héberger) qui vous permet d'ajouter votre déclaration, une case à cocher pour obtenir le consentement et un lien vers votre déclaration de confidentialité (que vous êtes chargé de rédiger et d'héberger). Ces deux liens doivent être saisis dans les paramètres du point de vente Internet.
- S-360 propose la fonction Amis et famille qui permet à un contact (le responsable d'un groupe) d'inclure des membres dans son groupe et d'effectuer certaines opérations au nom de ces membres (acheter des billets, payer des billets réservés, etc.). Cette fonctionnalité n'est disponible que si les membres ont donné leur accord. Ce nouveau comportement est activé par un paramètre au niveau de l'organisation :



Mandatory request consent for friend and family features yes no

Nous vous conseillons vivement d'activer ce paramètre pour vous conformer à la législation sur la protection de la vie privée. Seuls les clients qui utilisent déjà la fonction Friends & Family peuvent désactiver temporairement le consentement afin de disposer d'un peu de temps pour informer leurs internautes.

Même si les membres du groupe ont donné leur consentement, le responsable du groupe ne peut voir que les données qui sont directement nécessaires pour effectuer les différentes actions prévues par la fonction "Amis et famille". Par exemple :

- L'adresse électronique du membre du groupe n'est plus affichée.
- Les tickets du membre du groupe ne sont affichés que si le chef de groupe a le droit de les transférer (paramètre de configuration de la fonction Amis et famille).
- Les réservations du membre du groupe ne sont affichées que si le chef de groupe a le droit de payer les réservations (paramètre de configuration de la fonction Amis et famille).
- Lorsque le chef de groupe ajoute à ce groupe un contact qui n'existe pas encore dans la base de données du client final :
- Le chef de groupe ne pourra saisir que le minimum d'informations absolument nécessaires, laissant ainsi le choix aux membres du groupe de saisir des informations facultatives. Vous ne devez pas modifier le formulaire de création de contacts "Amis et famille" pour y ajouter des informations non essentielles.

- Les données concernant le membre du groupe seront supprimées si les membres du groupe ne donnent pas leur consentement après un certain nombre de jours (configurable).

En outre, nous vous rappelons que les clients qui effectuent une réservation par des canaux hors ligne doivent également être informés. Par conséquent, il vous incombe de veiller à ce que votre processus d'information pour chaque méthode de collecte de données soit conforme aux dispositions applicables en matière de protection des données (par exemple, dans les scripts des opérateurs ou sur un serveur vocal interactif pour les ventes par téléphone, et sur l'affichage au guichet).

En tout état de cause, vous avez l'obligation d'informer toutes les personnes concernées (différents types de contacts, opérateurs, fournisseurs, prospects, etc. dont les données peuvent figurer dans S-360), et pas seulement celles qui effectuent une réservation. De même, il est de votre responsabilité de vous en assurer et de mettre en place les processus nécessaires.

4.2.3 S-360 et vos opérateurs

4.2.3.1 Journaux d'audit et actions de l'opérateur

S-360 enregistre un journal d'audit et un journal des actions de l'opérateur. Les deux journaux sont automatiquement effacés au bout de 12 mois.

Le journal d'audit enregistre les modifications apportées à la configuration et permet de retrouver l'état antérieur des données. Ce type de journal est obligatoire dans certains pays à des fins comptables, par exemple pour déterminer si un prix de catalogue a été modifié.

Le journal des actions de l'opérateur enregistre les actions effectuées par les opérateurs. Il peut être utilisé par notre équipe d'assistance lorsqu'un incident est signalé afin de retrouver la séquence exacte des opérations.

4.2.3.2 Notifications sur les fonctionnalités de S-360

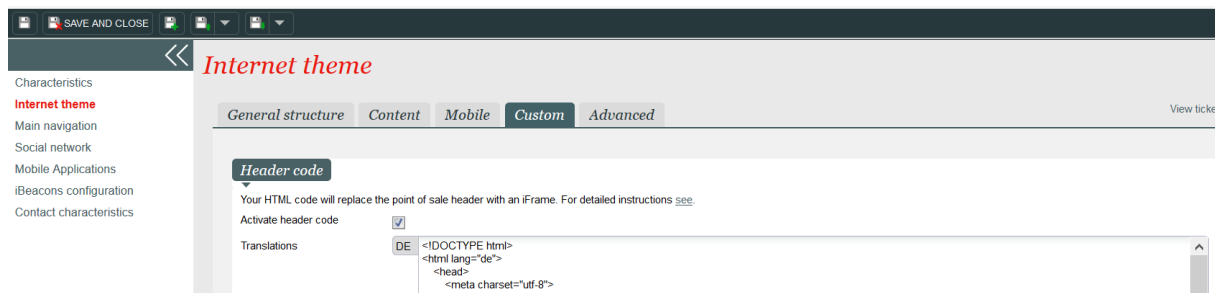
S-360 a récemment intégré un nouvel outil dans l'espace Note de Livraison du site web Confluence, appelé GetBeamer. Cet outil nous permet d'envoyer des messages sur nos notes de publication ou sur une fonctionnalité spécifique.

Le même outil a été intégré dans le module de back-office au cours du second semestre 2022.

GetBeamer fournit des statistiques sur la lecture de ces messages. Comme GetBeamer n'a pas accès au code de connexion ou au nom de l'opérateur, il identifie chaque opérateur avec un faux nom. Ces statistiques sont donc purement anonymes.

4.2.4 Personnalisation du Ticket Shop S-360

Le Ticket Shop S-360 peut être personnalisé de différentes manières. Par exemple, l'écran ci-dessous permet de remplacer l'en-tête standard par votre propre code HTML :



Le code HTML peut également être ajouté directement, c'est-à-dire sans utiliser le système S-360, par le biais de CSS.

Vous êtes seul responsable du respect du RGPD lorsque vous personnalisez notre Ticket Shop en y injectant du code, quelle que soit la technique utilisée. Par exemple, selon une décision récente d'une cour de justice allemande, vous ne devez pas utiliser les polices Google en appelant directement un service Google, car Google stockera l'adresse IP de votre client final et la conservera après avoir livré les polices. SECUTIX offre la possibilité de stocker les polices Google sur ses propres serveurs afin de protéger la vie privée de vos clients finaux.

4.3 La pertinence, l'adéquation et la stricte nécessité des données

4.3.1 Principes

Les données collectées et traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (cf. principe de minimisation de la collecte des données).

Vous ne pouvez collecter et traiter que les données nécessaires à la réalisation de la finalité (par exemple, les réservations, l'attribution des places ou le paiement de la commande). Étant donné que la réglementation précise qu'il est strictement interdit de collecter des données sans rapport avec la finalité du traitement, les personnes concernées doivent pouvoir choisir de fournir ou non des données non essentielles.

Il existe également certaines données particulièrement sensibles qui ne doivent pas être collectées ou traitées. En effet, par principe, il est interdit de collecter et de traiter les données suivantes

- Les "catégories particulières" de données 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 relatives à la santé ou les données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique.
- les informations relatives aux condamnations pénales et aux infractions ou aux mesures de sécurité connexes (telles que l'interdiction de stade).

Il existe des exceptions à ces interdictions. Par exemple, des "catégories particulières" de données peuvent être traitées si elles sont nécessaires au traitement et si l'une des conditions suivantes est remplie :

- La personne concernée a donné son consentement.

- Le traitement est effectué par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale (sous certaines conditions).
- La personne concernée a manifestement rendu les données publiques.

Néanmoins, ces exceptions doivent être interprétées de manière stricte.

Ces principes s'appliquent quelles que soient les méthodes utilisées pour collecter, saisir et traiter les informations contenues dans les outils. Les champs de commentaires ouverts, en particulier, doivent être utilisés avec prudence.

4.3.2 S-360

En tant que responsable du traitement des données, vous devez veiller au respect du principe de minimisation des données et du principe d'interdiction de collecter certaines données.

S-360 offre l'option de champs de collecte de données par défaut, que ce soit dans le back-office ou dans l'interface web ou le module web. Ces champs sont limités afin de minimiser les données. Dans le même temps, il convient de noter que :

- Il s'agit d'options de champs par défaut que vous pouvez modifier (à l'exception de certains champs strictement obligatoires pour que la solution fonctionne correctement, mais ceux-ci sont très limités - par exemple, les seules données strictement obligatoires pour les contacts sont la formule de politesse, le nom et le prénom). En tant que responsable du traitement, il vous incombe de déterminer les champs que vous utilisez ou ajoutez, conformément aux informations que nous vous demandons à l'annexe 1 afin de nous donner des instructions à cet égard.
- Il en va de même, par exemple, pour la définition des données "calculées" dans les caractéristiques de segmentation, que vous pouvez choisir de spécifier à l'annexe 1.

À cet égard, bien que S-360 vous donne accès à des fonctions de segmentation et éventuellement de profilage, vous êtes le seul décideur (et donc le seul responsable) des segments que vous souhaitez utiliser, des objectifs que vous poursuivez, de la pertinence, de l'adéquation et de la nécessité des données traitées dans ce contexte, des décisions que vous pouvez être amené à prendre concernant ces segments et des conséquences potentielles pour les personnes concernées.

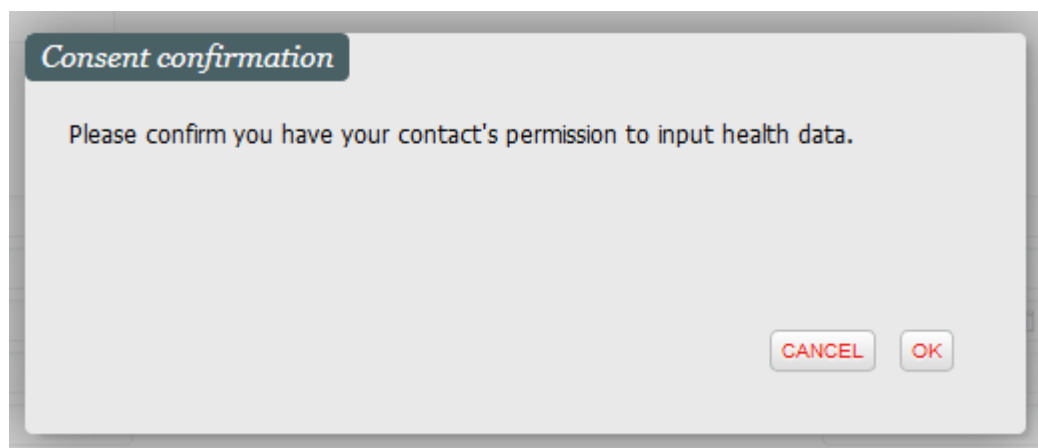
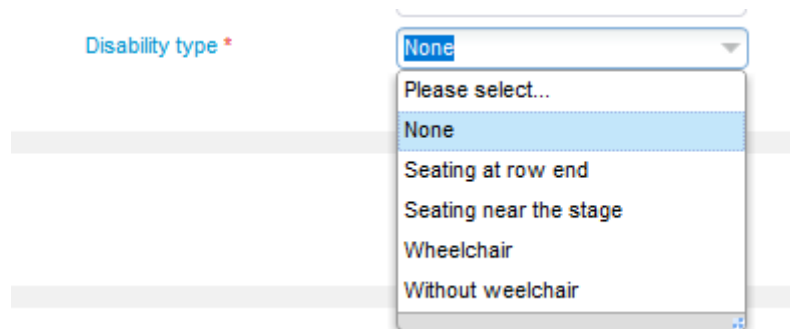
Notez également que la prise de décision individuelle automatisée au moyen, par exemple, de fonctions de segmentation ou, le cas échéant, de profilage peut faire l'objet de précautions particulières qu'il vous incombe de respecter (consentement, intervention humaine, possibilité de contester la décision, etc.)

- Les mêmes règles et principes s'appliquent au choix et à l'ajout de critères de reporting et d'extraction à l'aide des fonctionnalités de la solution. Par ailleurs, compte tenu des risques de données liés aux rapports et aux extractions une fois produits, nous vous recommandons de mettre en place une politique d'autorisation afin que seules les personnes ayant un intérêt strict puissent extraire des données (à préciser dans l'annexe 1).

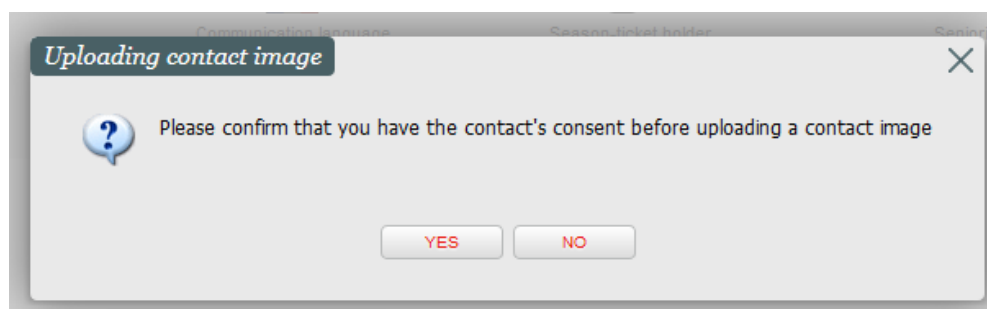
S-360 dispose également de certaines fonctionnalités destinées à vous permettre de respecter les principes applicables aux données collectées. C'est le cas par exemple:

- La valeur par défaut pour le handicap est "Pas de handicap". En outre, ce champ est configuré comme un menu déroulant qui limite les options de l'opérateur lors de la saisie des informations. Il s'agit de limiter le risque de collecter des données qui ne sont pas strictement nécessaires.

Pour entrer une autre valeur, l'opérateur de votre organisation doit confirmer qu'il a demandé le consentement du contact, comme suit :



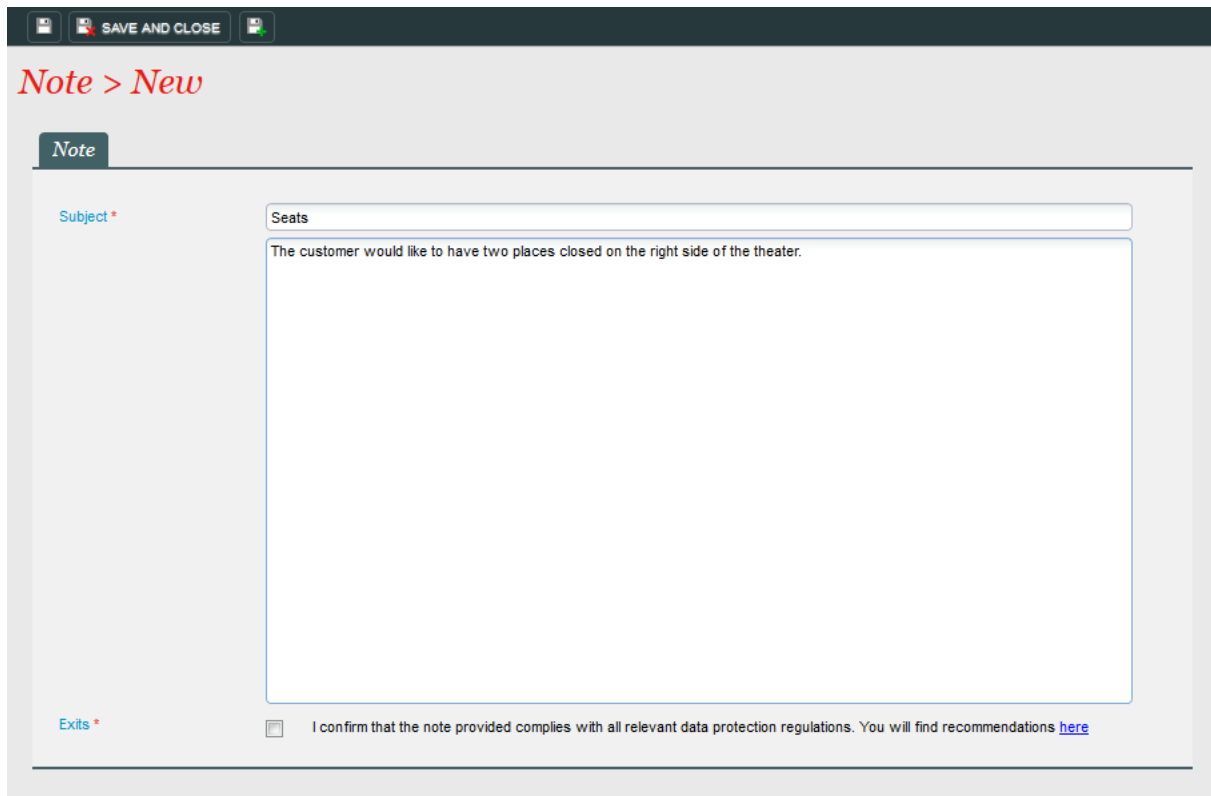
- Pour télécharger une photo, l'opérateur de votre organisation doit cocher une case pour confirmer qu'il a demandé le consentement du contact, comme suit :



Si vous autorisez le contact à télécharger sa photo sur le module web, vous devez ajouter ce consentement dans votre déclaration de confidentialité en ligne.

- S-360 ne stocke pas les données de la carte de paiement d'une personne en texte clair. En effet, seul un alias de carte est stocké. S-360 peut utiliser cet alias pour effectuer des paiements ultérieurs (exemple : paiement par carte de crédit en trois fois), mais l'alias ne permet pas d'effectuer d'autres paiements puisqu'il ne permet pas de trouver le numéro de la carte de crédit. La personne concernée doit donner son consentement avant le stockage de l'alias, que ce soit ou non :
 - la personne concernée coche une case dans l'interface ou le module web (non pré-cochée) ou
 - par un opérateur cochant une case dans le back-office (non pré-cochée et indiquant que le consentement explicite du contact est requis).

- Pour les champs de commentaires ouverts, l'opérateur de votre organisation doit cocher une case lors de la saisie des données pour confirmer que le commentaire est conforme aux dispositions applicables en matière de protection des données à caractère personnel. En outre, les opérateurs peuvent obtenir plus d'informations en cliquant sur un lien, comme suit :



SAVE AND CLOSE

Note > New

Note

Subject * Seats

The customer would like to have two places closed on the right side of the theater.

Exits * I confirm that the note provided complies with all relevant data protection regulations. You will find recommendations [here](#)

Recommended notes

Data entered in the notes area must comply with all relevant data protection regulations. Specifically, they must:

- Be relevant, adequate, not excessive and strictly relevant to the purpose for which they have been collected and processed;
- Be objective: not value judgements or opinions relating to the behaviour of the parties concerned; (to that end, you are advised to add strictly factual comments in finite sentences, avoiding the use of qualifiers).
- Avoid directly or indirectly revealing personal data such as racial or ethnic origins, political, philosophical or religious opinions, union affiliations; also avoid revealing data relating to genetic, biometric, health, sexual proclivity, or habits, criminal record or related security infringements.
- Avoid any expression which might be deemed offensive, derogatory, pejorative or detrimental to a person's reputation or infringe their personal privacy.

- Pour les champs de commentaires ouverts de l'interface web ou du module web affichés sur la page de finalisation d'une commande/réservation/option, il est de votre responsabilité de mettre en place la sensibilisation des opérateurs et les processus nécessaires à la modération de ces commentaires. En outre, un avertissement simplifié pour les contacts est inséré avec le texte par défaut :

"Les données saisies dans cette zone de commentaire ne doivent être utilisées que pour préciser les éléments strictement nécessaires à la passation et/ou à l'exécution de votre commande. Par ailleurs, nous vous rappelons que les informations que vous pouvez communiquer via cette zone de commentaire ouverte sont soumises aux dispositions applicables à la protection des données personnelles, que vous vous engagez à respecter (licéité, objectivité, pertinence, adéquation et limitation à ce qui est nécessaire au regard de la finalité poursuivie, loyauté de la collecte et du traitement des données...)."

- Les écrans de rapport et d'extraction comportent une mise en garde à l'intention des utilisateurs de S-360 :

Lorsque vous exportez ces données, vous devez vous assurer que vous agissez conformément à tous les principes applicables en matière de protection des

données à caractère personnel. En particulier, vous devez vous assurer que le fichier résultant ne sera utilisé que dans le prolongement du traitement initial et uniquement aux mêmes fins que celles poursuivies dans le cadre de la présente demande. Vous devez également vous assurer que les données récupérées sont pertinentes, adéquates et strictement nécessaires à la finalité pour laquelle vous comptez les utiliser, et ne les partager qu'avec les personnes autorisées. Il vous incombe de prendre toutes les mesures nécessaires pour garantir la sécurité et, en particulier, la confidentialité des informations. Le fichier d'exportation doit être conservé pendant une durée n'excédant pas celle prévue pour les données traitées dans le cadre de la présente demande.

- S-360 fournit une plate-forme ouverte qui simplifie l'intégration avec des systèmes externes, supprimant ainsi la nécessité de stocker des données sensibles sur S-360. Par exemple, si vous deviez appliquer les interdictions de stade décidées par les autorités officielles, au lieu de stocker ces informations sensibles directement sur S-360 avec tous les risques que cela implique, vous devriez envisager d'appeler une API fournie par cette autorité afin de vérifier si une personne concernée fait l'objet d'une telle interdiction. S-360 ne stockera qu'un identifiant personnel permettant d'identifier la personne concernée d'une manière sûre et non ambiguë. N'hésitez pas à contacter notre équipe service si vous rencontrez un tel problème.

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

4.4.1 Principes

S-360 vous permet d'analyser le comportement des utilisateurs en ligne à l'aide de Google Analytics. Votre organisation peut utiliser cette fonction, ou demander à SECUTIX SA de le faire en son nom, pour améliorer votre service. Elle mesure le nombre de visiteurs ainsi que les statistiques de navigation et de visite.

Les utilisateurs en ligne doivent être informés que vous utilisez des cookies de Google Analytics, et leur consentement est requis pour que nous puissions suivre leurs visites.

Pour ce faire, une bannière est affichée aux internautes qui visitent le site web (page d'accueil ou sous-page). Cette bannière offre les fonctionnalités suivantes :

- Il décrit brièvement les différents types de cookies et fournit un lien vers une explication détaillée mais facile à comprendre des catégories de cookies et des cookies au sein de chaque catégorie.
- Il permet de choisir entre refuser tous les cookies (sauf les plus importants), accepter tous les cookies ou choisir les catégories de cookies à accepter.
- L'internaute ne peut pas poursuivre sa navigation tant qu'il n'a pas choisi l'une des options décrites ci-dessus. En d'autres termes, le consentement ne peut être implicite

Aucun cookie ne peut être stocké sans le consentement de l'utilisateur.

Enfin, les utilisateurs qui donnent leur consentement à ce que vous stockiez ou lisiez des cookies doivent pouvoir le retirer à tout moment. Dans le cas où les personnes concernées donnent leur consentement, votre site doit le redemander après 13 mois dans tous les cas (cf. durée de vie maximale des cookies).

Pour votre information, il existe une dérogation à l'obligation d'obtenir le consentement pour les cookies de numéro de visiteur si les conditions suivantes sont remplies :

- L'utilisateur a été informé (cf. bannière).
- L'utilisateur a la possibilité de s'opposer à l'utilisation de ces cookies via un mécanisme facile à utiliser sur n'importe quel appareil, système d'exploitation, application ou navigateur. Vous ne devez pas collecter d'informations sur les personnes qui choisissent d'exercer leur droit d'opposition, ni les transmettre à l'éditeur de l'outil d'analyse de la fréquence des visites.
- L'objectif du cookie doit se limiter à mesurer le nombre de personnes qui consultent le contenu affiché afin d'évaluer à la fois le contenu lui-même et l'ergonomie du site ou de l'application.
- Les données collectées ne doivent pas être recoupées avec d'autres données traitées (par exemple des fichiers clients ou des statistiques de fréquentation d'autres sites). L'utilisation du cookie stocké doit être strictement limitée à la production de statistiques anonymes. Son champ d'application doit être limité à un seul éditeur et ne doit pas permettre de suivre les utilisateurs lors de l'utilisation d'autres applications ou sites web.
- Les données collectées ne peuvent être transférées que vers des pays offrant un niveau adéquat de protection des données.
- Si votre organisation capture des adresses IP pour la géolocalisation, l'adresse ne doit pas fournir d'informations plus détaillées que la ville. L'adresse IP doit également être supprimée ou anonymisée après la géolocalisation afin d'éviter toute autre utilisation des données ou tout chevauchement avec d'autres informations personnelles.
- La durée de vie des cookies doit être limitée à 13 mois et ne peut être prolongée automatiquement lors de nouvelles visites. Les données collectées par le biais des cookies ne doivent pas être conservées plus de 13 mois.

Par exemple, si vous n'êtes pas sûr à 100 % que l'outil d'analyse web que vous souhaitez utiliser répond à toutes ces exigences, son utilisation doit faire l'objet d'un consentement explicite préalable.

4.4.2 S-360

En tant qu'éditeur de site web (que vous utilisiez notre interface web, ou que vous intégriez notre module web dans votre propre site), vous êtes responsable d'informer les internautes sur les cookies et de l'obtention de leur consentement pour les stocker et les lire.

En ce qui concerne cette question :

- Sur demande sur l'outil de support client de SECUTIX SA, vous pouvez demander à ce que notre interface et notre module web vous donnent la possibilité d'afficher une bannière d'information sur les cookies et un dialogue de

consentement aux cookies lors de la première visite d'un utilisateur sur le site. La formulation des informations sur cette bannière est de votre responsabilité. A toutes fins utiles, nous vous proposons le texte suivant, que vous pouvez modifier ou adapter en fonction des spécificités de votre propre site web :

Information on cookies and management of your privacy settings

This website uses cookies or similar technologies to provide services and offers tailored to your areas of interest and to enable us to compile visit statistics.

We won't set any cookie, except the essential cookies, without your explicit consent. You can either refuse all (non essential) cookies, accept them all or select which kinds of cookies you accept. Your preferences will be stored during 6 months. You can change them at any time by clicking on the link CHANGE PRIVACY SETTINGS at the bottom of each page.

You can find more detailed explanations on the [cookie description page](#).

Refuse all cookies
Accept selected cookies
Accept all cookies

Essential
 Audience measurement
 Customisation

Vous devez mettre en place ce type de bannière que vous utilisiez notre interface web ou que vous ayez intégré notre module web dans votre site web. La bannière doit être configurée pour apparaître sur n'importe quelle page du site sur laquelle l'utilisateur arrive, même s'il s'agit d'une sous-page et non de la page d'accueil.

- Si vous n'utilisez pas la bannière S-360 décrite ci-dessus et mettez en place votre propre bannière, vous devez vous assurer que le choix effectué par l'internaute est accessible à notre interface web afin qu'il soit enregistré . Veuillez contacter notre équipe de service pour discuter des aspects techniques.
- Vous êtes responsable de la rédaction de votre politique en matière de cookies. Les cookies que nous utilisons dans le cadre de notre interface web sont décrits dans <https://confluence.secutix.com/display/DOCEN/List+des+cookies+utilisés+sur+c+e+site>.
 Vous devez inclure ces informations dans votre politique en matière de cookies.
 Vous devez mettre en œuvre ce type de politique en matière de cookies, que vous utilisiez notre interface web ou notre module web intégré à votre site web.
- En principe, vous ne devez pas placer de cookies sans le consentement explicite du visiteur (à l'exception des cookies essentiels au traitement de la commande), et la bannière doit réapparaître 13 mois après que vous avez obtenu leur consentement à l'utilisation de cookies. Il s'agit de la configuration par défaut mise en place par SECUTIX SA après votre demande de service. Si vous utilisez notre module intégré, vous devez vous assurer du respect de cette obligation sur votre propre site.
- Si vous souhaitez exempter votre organisation de l'obligation d'obtenir un consentement (afin de placer des cookies à partir de la page d'accueil), vous devez configurer les cookies conformément aux principes énoncés ci-dessus concernant les cookies relatifs au nombre de visiteurs qui ne sont pas soumis au consentement. Par exemple, si vous opérez en France, vous pouvez trouver une

liste d'outils d'analyse web exemptés de consentement sur <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-d'audience>.

Vous devez également respecter les autres obligations requises pour l'exemption de consentement.

Attention, cette exception au consentement n'est acceptée que pour les cookies de mesure d'audience : l'utilisation d'autres cookies tels que les cookies de réseaux sociaux ou les cookies publicitaires nécessite un consentement préalable de l'utilisateur.

4.5 Période de conservation des données

4.5.1 Principes

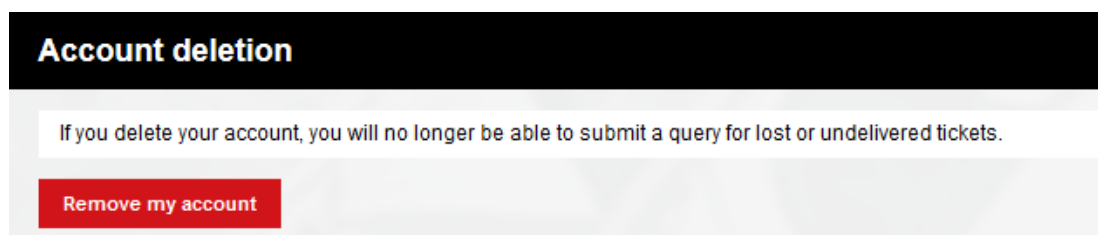
Les dispositions relatives à la protection des données à caractère personnel imposent aux responsables du traitement de conserver les données pendant une durée n'excédant pas celle qui est proportionnelle aux finalités poursuivies. Toutefois, elles ne donnent aucune indication quant à la durée exacte de conservation. Le stockage indéfini de données à caractère personnel n'est en aucun cas autorisé.

4.5.2 S-360

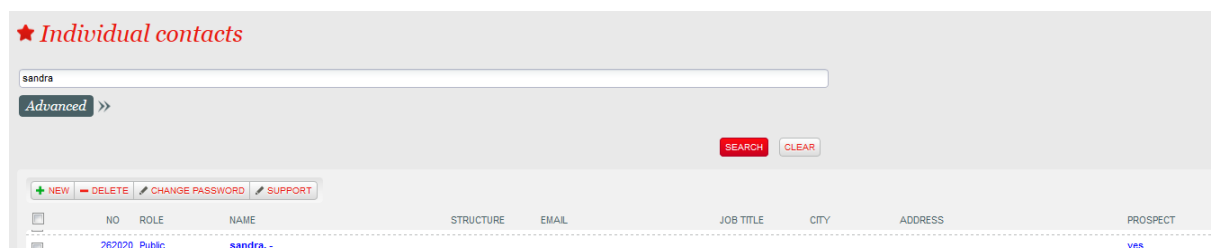
En tant que responsable du traitement des données, il vous incombe de spécifier et d'appliquer une durée maximale de conservation des données dans les outils que vous utilisez pour traiter les données à caractère personnel, en particulier dans S-360. Ce maximum s'applique à toutes les personnes concernées dont les données sont collectées et traitées dans S-360.

S-360 offre plusieurs fonctions de suppression des données :

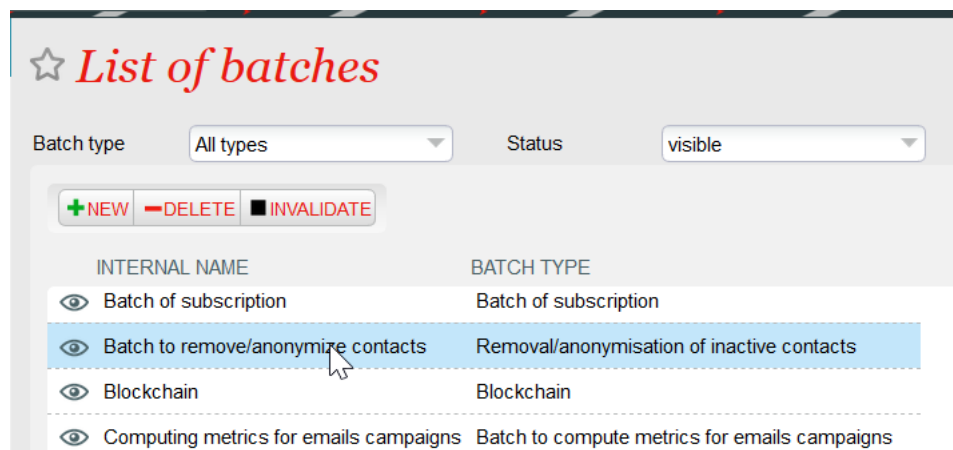
- Les contacts disposant d'un compte personnel en ligne peuvent supprimer leurs données à partir de ce compte :



- Les opérateurs de votre organisation peuvent supprimer des contacts :



- Dans les deux cas, le compte du contact et les informations marketing (historique et indicateurs) sont supprimés et toutes les commandes sont anonymisées. L'anonymisation des données devient irréversible lorsque les journaux sont supprimés, c'est-à-dire après 12 mois (voir la période de conservation des journaux).
- Les opérateurs de votre organisation peuvent supprimer des prospects.
- Les opérateurs de votre organisation peuvent anonymiser manuellement les données de toute personne concernée.
- S-360 dispose également d'une fonction vous permettant, en fonction de vos choix, de vos habitudes, de votre secteur d'activité et des réglementations en vigueur, de détecter les contacts inactifs depuis *une durée de plus de x* mois et de les supprimer/anonymiser par lots :



- Après avoir défini l'état d'un opérateur comme étant "suspendu", vous pouvez anonymiser l'opérateur en remplaçant simplement son nom, prénom, adresse email, etc. par XXXX. L'anonymisation des données devient définitive lorsque les logs techniques sont supprimés, c'est-à-dire après 12 mois (cf. délai de conservation des logs). Attention, il n'est pas possible de modifier/anonymiser le code de connexion des opérateurs. Ainsi, les administrateurs qui créent des opérateurs sont responsables de s'assurer qu'ils n'introduisent pas d'informations permettant d'identifier la personne.
- S-360 génère différents documents et courriels dont la durée de conservation est mentionnée à l'annexe 3. Il convient de noter que ces documents peuvent contenir des données personnelles, notamment le nom et l'adresse de la personne concernée.

Dans tous les cas, à la fin du contrat, vos données seront récupérées et vous seront renvoyées dans le dernier format standard de l'industrie. Elles sont ensuite supprimées de S-360 et sont soumises aux mêmes règles de purge que pour la suppression manuelle (cf. ci-dessus).

4.6 Des données exactes et à jour. Droits d'accès, de rectification, d'effacement et de portabilité. Droits de restriction du traitement et d'opposition.

4.6.1 Principes

En vertu des dispositions applicables en matière de protection des données à caractère personnel, les données traitées sont exactes et, si nécessaire, mises à jour. Les responsables du traitement prennent les mesures appropriées pour que les données inexactes au regard des finalités pour lesquelles elles sont traitées soient effacées ou rectifiées.

Les personnes concernées se voient garantir le droit d'accès à leurs données, le droit à la portabilité de leurs données et le droit à la rectification et à l'effacement de leurs données.

En outre, ils ont le droit de restreindre le traitement de leurs données et/ou de s'y opposer.

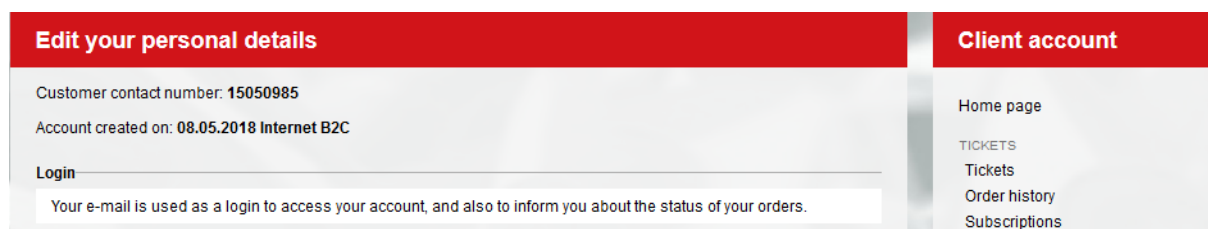
Ces obligations incombent au responsable du traitement des données. Toutefois, le sous-traitant des données doit fournir l'aide nécessaire au responsable du traitement des données pour s'acquitter de son obligation de répondre aux demandes des personnes concernées qui souhaitent exercer leurs droits.

4.6.2 S-360

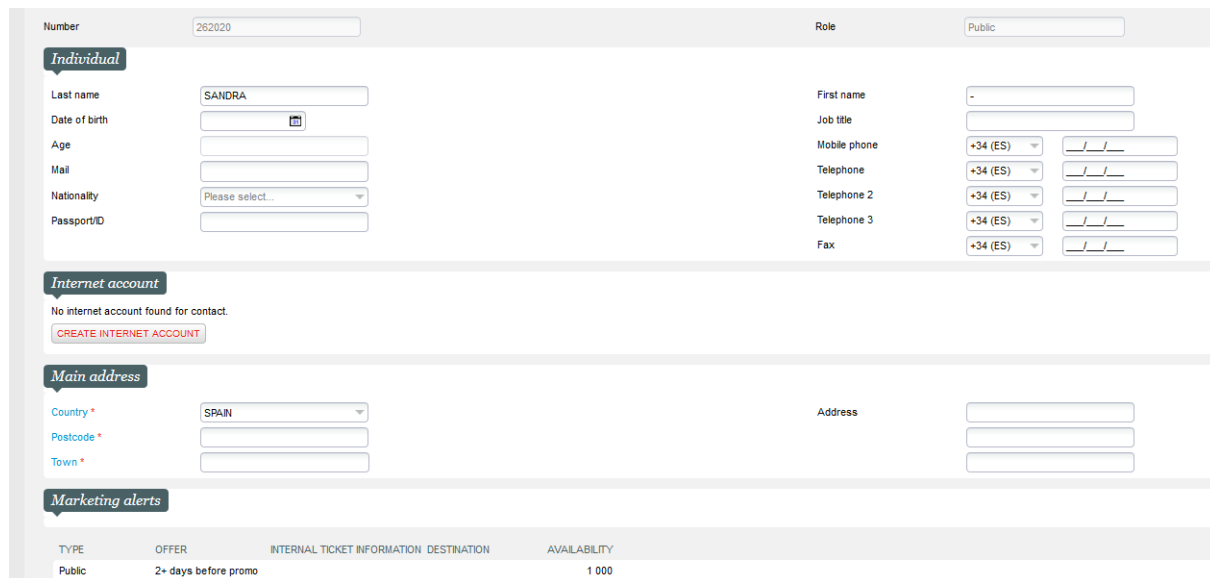
Lorsque les personnes concernées exercent ces droits, vous devez, en tant que responsable du traitement, veiller à leur fournir les réponses prévues par les dispositions applicables et à donner suite à leurs demandes (pour autant qu'elles remplissent les conditions requises). A cet égard, notez que nous vous indiquerons si une demande nous est adressée directement, mais la réponse et les démarches nécessaires restent de votre seule responsabilité.

S-360 comprend des fonctionnalités conçues pour gérer les demandes de rectification et d'effacement des données contenues dans la base de données S-360.

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



- Les opérateurs de votre organisation peuvent mettre à jour les fichiers de contacts :



TYPE	OFFER	INTERNAL TICKET INFORMATION	DESTINATION	AVAILABILITY
Public	2+ days before promo			1 000

- Voir le paragraphe 4.5 pour des informations sur les demandes d'effacement de données.

Lorsqu'ils exercent leurs droits d'accès aux données ou de portabilité, les contacts peuvent demander toutes les informations personnelles que vous détenez sur eux. Les opérateurs de votre organisation ont accès aux données des contacts pour répondre à ces demandes. Ils peuvent également obtenir l'ensemble des informations stockées sur un contact (fiche contact, historique des achats, historique des relations) en adressant une demande à SECUTIX SA.

En outre :

- La source d'information dans le fichier de contact est indiquée. Les valeurs possibles sont les suivantes :
 - **IMPORT** : informations collectées via l'importation de données, par exemple la migration de données au cours de l'intégration.
 - **BACKOFFICE** : informations saisies par un opérateur de votre organisation en dehors du contexte d'une réservation ou d'une vente.
 - **Type de canal de vente** : Informations introduites à partir d'un canal de vente du type spécifié. Le type mentionné vous indique si l'information a été saisie par un utilisateur final (exemple : canal de vente B2C sur internet), par un opérateur de votre organisation (exemple : billetterie) ou par un opérateur externe (exemple : canal de vente B2B2C).

☆ *Contact individual > 262020 Dear Sir or Madam - sandra (Prospect)*

Summary General Marketing Management Notes Administration

Created from	IMPORT	Date inserted	25/07/2016
User Inserted	IMPCTCT_SERV-240	Date Updated	15/08/2017
User Updated	STX-73980-pre		

- La date de création des comptes personnels est disponible auprès du compte concerné :

Edit your personal details

Customer contact number: **28**

Account created on: **14.11.2012**

Login _____

Your e-mail is used as a login to access your account, and also to inform you about the status of your orders.

- La date de création et la date de dernière modification de la fiche contact sont indiquées dans le fichier :

☆ *Contact individual > 262020 Dear Sir or Madam - sandra (Prospect)*

Summary General Marketing Management Notes **Administration**

Created from	IMPORT	Date inserted	25/07/2016
User inserted	IMPCTCT_SERV-240	Date Updated	15/08/2017
User Updated	STX-73980-pre		

En fin de compte, vous êtes responsable de la gestion des demandes de restriction du traitement des données et des objections.

En tout état de cause, nous nous engageons à vous fournir tous les éléments de données que nous détenons, sur demande, pour vous permettre de répondre aux personnes concernées qui souhaitent exercer leurs droits, et nous mettrons à votre disposition les ressources nécessaires.

4.7 Sécurité des données

4.7.1 Principes

Compte tenu de l'état de la technique, du coût de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques de probabilité et de gravité variables que présente le traitement 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 pour garantir un niveau de sécurité adapté au risque, y compris, entre autres, le cas échéant :

- La capacité à assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement.
- La capacité à rétablir la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique.

- un processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles destinées à garantir la sécurité du traitement.

Vous devez donc mettre en œuvre des mesures de sécurité et de confidentialité adéquates. Pour des recommandations sur la sécurité des données, consultez : <https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles> (version française) ou <https://www.cnil.fr/en/gdpr-developers-guide> (version anglaise).

Lorsqu'un type de traitement utilisant notamment les 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 procède, avant le traitement, à une évaluation de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

En cas de violation de données à caractère personnel (violation de la sécurité entraînant accidentellement ou illégalement la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel traitées ou l'accès non autorisé à de telles données), le responsable du traitement notifie cette violation à l'autorité de contrôle dans les meilleurs délais et, dans la mesure du possible, au plus tard 72 heures après en avoir pris connaissance. Lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement en informe la personne concernée dans les meilleurs délais.

4.7.2 S-360

En tant que responsable du traitement des données, vous devez vous assurer que vous respectez toutes ces obligations.

En tant que sous-traitant, SECUTIX SA est responsable du déploiement des mesures de sécurité appropriées, de la notification au responsable du traitement de toute violation de données à caractère personnel dans un délai raisonnable après en avoir pris connaissance et, plus généralement, a l'obligation de coopérer avec le responsable du traitement afin de lui permettre de se conformer à ses obligations (en particulier, le déploiement de mesures de sécurité appropriées et l'évaluation de l'impact).

SECUTIX SA garantit de répondre aux exigences et d'obtenir les certificats de conformité aux normes ISO/IEC 27001:2013, ISO 27701:2019 et PCI DSS v3.2. Ainsi, SECUTIX SA s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles identifiées dans ces normes.

En outre, en ce qui concerne S-360 :

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

antivirus actuels, le cryptage SSL et la journalisation lors de la modification manuelle des bases de données.

- La composante financière de S-360 est certifiée PCI DSS et fait l'objet d'un audit une fois par an.
- Pour être valables, les mots de passe doivent comporter un chiffre et une combinaison sûre de caractères et de chiffres.
- S-360 fournit un processus d'authentification à deux facteurs pour les opérateurs du back-office et de la billetterie. SECUTIX vous conseille vivement d'activer cette fonction qui réduit considérablement le risque d'accès non autorisé à vos données, y compris les données personnelles. Vous trouverez plus d'informations sur cette fonctionnalité sur <https://confluence.secutix.com/display/RN/Two+factor+authentication+for+operators>.
- S-360 fournit un processus de création d'opérateur sûr dans lequel l'opérateur créateur ne définit pas le mot de passe de l'opérateur créé, mais lui envoie un courriel avec un lien pour définir le sien. Bien que ce processus exige que chaque opérateur ait sa propre adresse électronique, nous vous recommandons vivement de l'activer. Vous trouverez plus d'informations sur <https://confluence.secutix.com/display/RN/More+procédure+sécurisée+pour+créer+de+nouveaux+opérateurs>.
- S-360 dispose d'un plan de continuité pour le passage d'un centre de données à un autre.
- L'accès physique aux centres de données est strictement contrôlé par des codes, un système de suivi, des alarmes, des badges et la télévision en circuit fermé.
- Les données envoyées au site de sauvegarde sont cryptées via VPN ou HTTPS.

En outre, dans le respect de nos obligations, nous nous engageons à coopérer avec vous en vue de :

- vous permettre de respecter vos propres obligations en matière de sécurité et, en particulier, de confidentialité des données à caractère personnel.
- vous permettre de réaliser des analyses d'impact sur le traitement des données à caractère personnel si la nature du traitement auquel nous participons l'exige, et de consulter l'autorité de contrôle, le cas échéant, au sujet de ce traitement
- respecter votre obligation de notifier l'autorité de contrôle et d'informer 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 aurons connaissance. Nous nous engageons également à utiliser tous les moyens à notre disposition et à vous communiquer, à votre demande, toute documentation que nous détenons et qui vous serait utile pour effectuer ces notifications.

Vous devez également prendre les mesures techniques et organisationnelles internes appropriées pour garantir un niveau de sécurité adéquat pour les données traitées dans S-360. Par exemple, nous vous recommandons de

- sauvegarder et maintenir l'accès actuel à S-360 (matériel, logiciel, réseau, accès à l'internet)

- s'assurer de la confidentialité des mots de passe utilisés par les opérateurs de votre organisation pour se connecter à S-360, et veiller à la mise en place d'une politique de mots de passe conforme aux recommandations applicables (cf. à titre indicatif les recommandations disponibles ici : <https://www.cnil.fr/en/passwords-minimum-security-recommendations-businesses-and-citizens> (version anglaise) ou <https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite> (version française)). En conséquence, les différents opérateurs de votre organisation ne doivent jamais partager le même login S-360.
- activer le processus d'authentification à deux facteurs pour les opérateurs
- nettoyer systématiquement les profils opérateurs (supprimer leurs droits d'accès lorsqu'ils quittent l'entreprise)
- maintenir les programmes antivirus à jour sur tous les postes de travail
- etc.

4.8 Sous-traitants des données et transferts transfrontaliers

4.8.1 Principes

Les responsables du traitement qui font appel à des sous-traitants et/ou des sous-traitants ultérieurs pour traiter des données à caractère personnel doivent le faire dans un cadre contractuel spécifique qui comprend certaines clauses obligatoires.

Les flux transfrontaliers de données à caractère personnel vers des États non-membres de l'UE/EEE et/ou non reconnus par la Commission européenne comme offrant un niveau de protection adéquat ne seront mis en œuvre que s'ils sont soumis à des garanties contractuelles suffisantes. .

4.8.2 S-360

Dans le cadre de la prestation de services de S-360, nous devons traiter des données personnelles au nom de votre organisation, ce qui signifie que nous agissons en tant que responsable du traitement des données. Les documents contractuels que nous fournissons à cette fin comprennent une clause décrivant nos services dans ce rôle de responsable du traitement des données, conformément aux exigences du GDPR.

Étant donné que nous fournissons la solution, diverses entités de notre groupe doivent traiter les données à caractère personnel en votre nom. À cet égard, notez que les entités de notre groupe sont principalement basées dans l'Union européenne ou en Suisse, ce qui garantit un niveau adéquat de protection des données. Toutefois, une entité est basée au Vietnam. Conformément aux dispositions applicables en matière de protection des données, les flux transfrontaliers de données vers cette entité sont régis par l'accord sur les clauses contractuelles types du groupe ELCA (maison-mère de SECUTIX S.A.), basé sur les modèles établis par la Commission européenne et révisé selon les directives du Préposé fédéral suisse à la protection des données et à la transparence (PFPDT).

En outre, en fonction des services inclus dans votre abonnement, afin de vous fournir toutes les fonctionnalités offertes dans le cadre de S-360, nous devons faire appel à des sous-traitants supplémentaires. Ceux-ci sont énumérés à l'annexe 2.

4.9 Utilisation des données à des fins de marketing

4.9.1 Principes

En ce qui concerne l'utilisation des données à des fins de marketing, les principes suivants s'appliquent :

- Les personnes concernées doivent donner leur consentement exprès (en cochant une case vide accompagnée d'un texte invitant la personne concernée à donner son consentement) pour recevoir des courriels, des sms, et des communications électroniques automatisées (cf. appels automatisés).
- Les personnes concernées ne doivent pas avoir préalablement refusé les communications par courrier postal ou les contacts téléphoniques avec intervention humaine.
- Chaque communication envoyée (en particulier par courrier électronique et par SMS) doit comporter un moyen simple et gratuit de se désinscrire (droit d'opposition) des communications effectuées par le canal concerné, et l'objet des courriers électroniques doit se rapporter au contenu du courrier électronique et préciser au nom de qui il est envoyé.

En ce qui concerne les courriels ou les sms, il convient de noter qu'une dérogation à l'obligation de consentement peut être exercée si toutes les conditions suivantes sont remplies :

- Les coordonnées du destinataire ont été collectées lors d'une vente ou d'une prestation de service.
- La communication est conforme aux dispositions applicables en matière de protection des données à caractère personnel, notamment en ce qui concerne les informations sur les individus.
- La prospection directe concerne des produits ou services similaires fournis par la même personne physique ou morale.
- Les destinataires ont expressément et clairement la possibilité de s'opposer facilement et sans frais (à l'exception des frais liés à l'envoi de l'opposition) à l'utilisation de leurs coordonnées au moment où celles-ci sont collectées et chaque fois que le contact reçoit un courrier électronique de prospection.

4.9.2 S-360

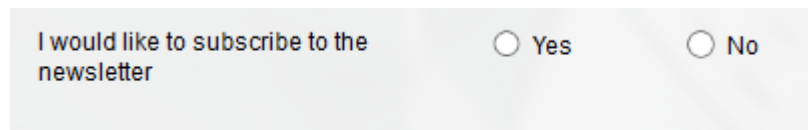
S-360 comprend des fonctionnalités marketing qui vous permettent d'envoyer des messages promotionnels à vos contacts (clients et prospects). Toutefois, l'utilisation de ces fonctionnalités relève de votre seule responsabilité et vous devez vous conformer aux principes énoncés ci-dessus.

Pour vous permettre de mener vos activités de marketing dans le respect de ces principes, SECUTIX SA a mis en place les dispositifs suivants :

- Le formulaire mis à disposition des internautes pour créer un compte personnel en ligne via notre interface ou module web comporte un encart pour la déclaration

dont la rédaction vous incombe. Vous devez remplir la déclaration en utilisant des cases à cocher vides et les mentions obligatoires informant les utilisateurs que leur consentement est requis/qu'ils peuvent s'opposer à l'utilisation de leurs données. Ces éléments doivent être introduits dans les paramètres du point de vente internet.

- Les utilisateurs en ligne disposent de plusieurs fonctions par défaut dans leur compte personnel en ligne :
 - S'abonner ou se désabonner de la (des) lettre(s) d'information (adaptable(s) à vos besoins) :



I would like to subscribe to the newsletter Yes No

- Un choix de canaux de communication et d'expéditeurs (adaptable à vos besoins) :

	I accept	I refuse
I would like to receive all the latest news and happenings by e-mail: events calendar, ticket sales alerts, new products, etc. *	<input type="radio"/>	<input checked="" type="radio"/>
I would like to receive exclusive offers by SMS. *	<input type="radio"/>	<input checked="" type="radio"/>
I accept that my details be transmitted to third-party partners. *	<input type="radio"/>	<input checked="" type="radio"/>

Lorsque les internautes acceptent de recevoir des communications (c'est-à-dire qu'ils ont choisi "Je souhaite recevoir toutes les dernières nouvelles et tous les événements par courrier électronique..."), ils recevront un courriel de confirmation de leur consentement contenant un lien leur permettant de confirmer leur consentement. Ce n'est qu'à ce moment-là qu'ils recevront des communications. .

- S-360 vous permet de recueillir le consentement à recevoir certaines lettres d'information de la part de vos partenaires. Ce consentement est également soumis à un double opt-in (e-mail de confirmation). Vous pouvez ensuite envoyer la liste des contacts qui ont donné leur consentement à votre partenaire. Notez que votre partenaire est responsable de la gestion des opt-outs. Vous trouverez plus d'informations sur cette fonctionnalité sur <https://confluence.secutix.com/display/RN/Gather+consentement+au+cœur+de+votre+promoteurs+ou+organisateur+d'événements> .
- S-360 permet d'informer vos clients dans le cadre d'une obligation contractuelle, sans qu'il soit nécessaire de recueillir leur consentement. Un exemple typique est d'informer qu'un événement a été annulé ou retardé. Vous êtes seul responsable de l'utilisation de cette fonction uniquement pour répondre à des obligations contractuelles. SECUTIX SA se réserve le droit de vérifier et d'identifier les abus potentiels (envoi d'informations marketing au lieu d'informations contractuelles) et de bloquer l'envoi d'e-mails manifestement abusifs.
- Au guichet (dans l'arrière-boutique) :

- Les opérateurs de votre organisation peuvent préciser si un contact est prêt à recevoir des communications de votre organisation, de ses partenaires et de tiers.

Legal information

Accept communication from institution	<input type="radio"/> yes <input type="radio"/> no
Accepts transmission of elec. coordinates to third parties	<input type="radio"/> yes <input type="radio"/> no
Accept communication from one partner	<input type="radio"/> yes <input type="radio"/> no

- Vos opérateurs peuvent spécifier les canaux de communication que le contact préfère :

Communication

Preferred channel	<input type="text" value="SMS/MMS"/>
Preferred moment	<input type="text" value="Weekday"/>
SMS_MMS	<input checked="" type="radio"/> yes <input type="radio"/> no
Telephone	<input checked="" type="radio"/> yes <input type="radio"/> no
Email	<input checked="" type="radio"/> yes <input type="radio"/> no
Letter	<input checked="" type="radio"/> yes <input type="radio"/> no
Bounce status *	<input type="text" value="Valid"/>

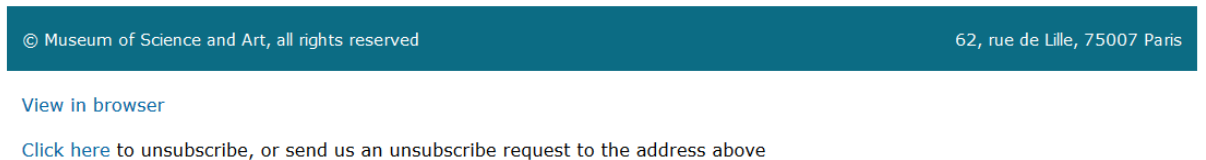
- Toutes les cases sont vides par défaut. De même, l'opt-in nécessite une action positive de la part du visiteur en ligne ou d'un opérateur. Vous devez tenir compte de ces règles de gestion afin de mener vos activités de marketing dans le respect des principes énoncés au paragraphe 4.9.1.

Vous devez également tenir compte des demandes d'opposition à la prospection qui sont portées à votre attention par les personnes concernées (en cochant "non" pour les canaux de communication en question).

En résumé, vous devez tenir compte des principes suivants :

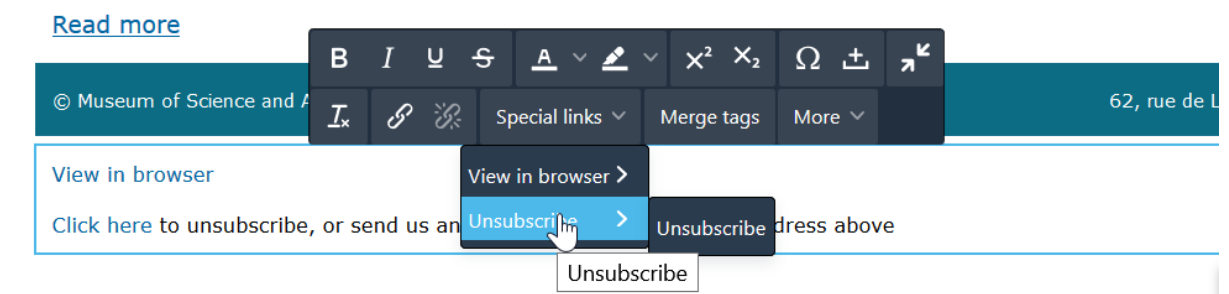
- Vous ne devez pas prospecter un contact via un canal de communication marqué "non".
- Vous ne pouvez prospecter que par courrier électronique, sms, mms, fax ou systèmes automatisés de communication électronique via un canal de communication marqué "oui"
- Vous pouvez prospecter par courrier ou faire du télémarketing via un canal de communication marqué "oui" ou laissé vide (cf. ni "oui" ni "non").

Les lettres d'information que S-360 envoie à votre demande contiennent au minimum des informations permettant aux destinataires d'exercer leur droit d'opposition (c'est-à-dire qu'ils souhaitent ne plus recevoir de communications de ce type). Ces communications comportent un lien de désinscription. La désinscription est automatiquement prise en compte dans S-360 (le système met la case "non") :



Pour inclure cette fonctionnalité dans les courriels que vous envoyez, veuillez inclure l'une des deux solutions ci-dessous dans leur configuration :

- L'opérateur de votre organisation configure le lien "Unsubscribe URL". Les contacts sont automatiquement désinscrits lorsqu'ils cliquent sur le lien :



- L'opérateur de votre organisation ajoute un lien qui redirige les contacts vers leur espace personnel, où ils peuvent se désabonner ou modifier leurs préférences.

4.10 Formalités

4.10.1 Principes

Les responsables du traitement des données tiennent un registre des activités de traitement sous leur responsabilité.

Les responsables du traitement des données tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte des responsables du traitement des données.

Ces enregistrements se font par écrit, y compris sous forme électronique. Le responsable du traitement des données ou le sous-traitant des données met le registre à la disposition de l'autorité de contrôle sur demande.

4.10.2 S-360

En tant que responsable du traitement des données, vous devez intégrer le traitement des données à caractère personnel mis en œuvre à l'aide de S-360 dans votre registre des activités de traitement du "responsable du traitement des données".

En tant que responsable du traitement des données, nous devons intégrer le traitement des données à caractère personnel effectué en votre nom à l'aide du logiciel S-360 dans notre registre des activités de traitement.

Annexe 1 Liste de contrôle à remplir par votre organisation concernant le traitement des données à caractère personnel effectué à l'aide de S-360

Question	Réponse	Remarques
Finalités pour lesquelles votre organisation utilise la solution et les services inclus dans votre abonnement		Objectifs poursuivis, fonctionnalités de l'application choisies, utilisations effectives ou prévues, finalités répondant à des dispositions spécifiques, conséquences du traitement,...
Données collectées et traitées dans la solution	...	Détails des données que le client souhaite collecter et traiter lors de l'utilisation de S-360
Personnes autorisées à ajouter de nouveaux champs + méthode utilisée pour en faire la demande à SECUTIX SA		Communiquer l'identité des personnes autorisées chez le client + préciser comment les demandes peuvent être adressées à SECUTIX SA
Personnes autorisées à ajouter de nouveaux critères de segmentation + méthode utilisée pour en faire la demande à SECUTIX SA		Communiquer l'identité des personnes autorisées chez le client + préciser comment les demandes peuvent être adressées à SECUTIX SA
Personnes autorisées à ajouter de nouveaux critères de signalement/récupération + méthode utilisée pour en faire la demande à SECUTIX SA		Communiquer l'identité des personnes autorisées chez le client + préciser comment les demandes peuvent être adressées à SECUTIX SA
Destinataires des connexions "administrateur		Il appartient alors au client de déterminer et de configurer lui-même les personnes pouvant avoir accès aux données, ainsi que le détail des autorisations aux données, écrans, fonctionnalités (ex : consultation, saisie, reporting/extraction,...).
Durée de conservation des données souhaitée dans la solution		S-360 permet de définir la durée de conservation des données, ce qui donne au client les moyens de fixer lui-même la durée souhaitée.
Contact organisationnel au cas où les personnes concernées souhaiteraient exercer leurs droits		Communiquer l'identité et les coordonnées du client

Contact organisationnel en cas de violation de données	Communiquer l'identité et les coordonnées du client
Personne de référence pour la protection des données	Communiquer l'identité et les coordonnées du délégué à la protection des données du client, ou au moins du référent "protection des données personnelles".
Autres instructions de l'organisation à SECUTIX SA	Préciser toute autre instruction du client à l'attention de SECUTIX SA

Annexe 2 Liste des sous-traitants de SECUTIX SA

La liste des sous-traitants de SECUTIX SA :

Sous-sous-traitant (Nom et adresse)	Finalité de la transmission (Description)	Données transmises (Liste détaillée)
ELCA Information Technology (Vietnam),Ltd Melody-2 Tower N1 Dien Bien Phu Binh Thanh District Ho Chi Minh City Vietnam	Section 10.1.3	Section 10.1.6

Annexe 3 Durée de conservation des documents

S-360 génère différents documents et courriels dont la durée de stockage sur est mentionnée dans le tableau ci-dessous. Notez que certains documents listés ci-dessous sont spécifiques à certaines fonctionnalités et peuvent ne pas être pertinents dans votre cas.

Identifiant du document	Description	Durée de stockage (années)
DOC_CLASSE/COMPTE_CRÉDIT_BANCAIRE	Note de crédit virement bancaire récapitulation	10
DOC_CLASS/ACCOUNT_BANKDEBIT	Note de crédit retrait bancaire récapitulatif	10
DOC_CLASSE/NOTIFICATION D'AVANTAGE	Courriel de notification d'avantage	2
DOC_CLASS/ARTIST_WAITLIST_EMAIL	Liste d'attente des artistes	1
DOC_CLASSE/CONFIRMATION_AUTORISATION	Confirmation de l'autorisation	1
DOC_CLASS/BVR	Résumé avec BVR	10
DOC_CLASSE/B2B_ACCOUNT	Confirmation de la création d'un compte B2B	2
DOC_CLASS/CAMPAIGN_EMAIL_BASIC	Courriel de base	2
DOC_CLASS/CAMPAIGN_EMAIL_ECOMM	Courrier électronique pour le commerce électronique	2
DOC_CLASS/CAMPAGNE_EMAIL_NEWSLET	Lettre d'information électronique	2
DOC_CLASSE/CAMPAGNE_SMS	Marketing SMS	2
DOC_CLASS/CANCEL_RESALE_ACK	Billet retiré de la notification de revente	1
DOC_CLASS/CGV	CGV (document de texte statique)	2
DOC_CLASSE/CODE_EMAIL	Liste de codes dans l'e-mail	2
DOC_CLASS/CONFIRM_PROD_WAITLIST_EMAIL	Confirmation liste d'attente produit	1
DOC_CLASS/CONFIRM_WAITLIST_EMAIL	Liste d'attente pour la confirmation	1
DOC_CLASSE/CONTACT	Document de contact	1
DOC_CLASS/CREDIT_NOTES	Reçu de la note de crédit	10
DOC_CLASS/EMAIL_CANCEL_CONFIRMATION	Courriel de confirmation d'annulation	2
DOC_CLASS/EMAIL_EXPIRED_OPTION	Options bientôt expirées	1
DOC_CLASS/EMAIL_FOLLOW_SHIPMENT	Suivre l'expédition	1
DOC_CLASS/EMAIL_OPTION_BOOKING_REMINDER	Rappel des options/réservations	1
DOC_CLASS/EMAIL_OPTION_WAIT_LIST	Options de liste d'attente	1
DOC_CLASS/EMAIL_REQUEST_REMINDER	Rappel préalable à la demande	1
DOC_CLASS/EMAIL_RESERVATION_REMINDER	Rappel des réservations	1
DOC_CLASS/EMAIL_TICKET_HOLDER_RESOLD	Notification des billets revendus pour le contact culturel	2
DOC_CLASS/EXCHANGE_TICKET_ACK	Billets d'échange	1
DOC_CLASSE/FILE_PROFORMA	Dossier pro forma	2
DOC_CLASSE/RÉSUMÉ_DE_FICHER	Récapitulatif des dossiers	10
DOC_CLASS/GOODS_ORDER	Bon d'achat	10

DOC_CLASS/INSTALLEMENT_PAYING_FAILURE	Courriel d'échec de paiement par acomptes	2
DOC_CLASS/INSTALLEMENT_PAYING_SUCCESS	Courriel de réussite du paiement échelonné	2
DOC_CLASS/INSTALLEMENT_REMINDER	Courriel de rappel des versements	1
DOC_CLASSE/LETRE	Lettre d'accompagnement	2
DOC_CLASSE/NOUVEAU_COMPTE	Courriel de création de compte	2
DOC_CLASS/OPTION_ORDER_ACK	Confirmation de la commande d'options	2
DOC_CLASS/OPTION_REQUEST_ACQUITTEMENT	Demande d'option ack/acquittement	2
DOC_CLASS/OPTION_REQUEST_DELETION	Demande d'annulation d'option ack/acquittement	2
DOC_CLASS/OPTION_REQUÊTE_MODIFICATION	Modification de la demande d'option ack/acquittement	2
DOC_CLASS/OPTION_SUMMARY	Récapitulation des options et des refus	2
DOC_CLASSE/ACCUSÉ DE RÉCEPTION DE COMMANDE	Ack/accusé de réception de la commande	1
DOC_CLASS/ORDER_ACK_WITH_CONF	Ack/accusé de réception de la commande avec confirmation	5
DOC_CLASSE/ORDRE_DE CRÉDIT BANCAIRE	Récapitulatif de l'ordre de virement bancaire	5
DOC_CLASS/ORDER_BANKDEBIT	Récapitulatif de l'ordre de retrait bancaire	5
DOC_CLASS/CONFIRMATION_DE COMMANDE	Confirmation de commande	2
DOC_CLASSE/RÉSUMÉ DU FICHER DE COMMANDE	Récapitulatif de la commande (état actuel)	10
DOC_CLASS/ORDER_INVOICE	Commande de la facture	10
DOC_CLASSE/ORDRE REJETÉ	Refus de commande	2
DOC_CLASSE/RÉSUMÉ DE LA COMMANDE	Récapitulation de la commande (état statique)	10
DOC_CLASSE/PARTENAIRE	Partenaire	10
DOC_CLASS/PASSWORD_CHANGE	Changement de mot de passe	1
DOC_CLASS/PASSWORD_RESET	Réinitialiser le mot de passe	1
DOC_CLASSE/CONFIRMATION_DE PAIEMENT	Avis de paiement échelonné	2
DOC_CLASS/PRODUCT_WAITLIST_EMAIL	Liste d'attente des produits	1
DOC_CLASSE/PROFFORMA	Dossier pro forma	1
DOC_CLASS/PUT_ON_RESALE_ACK	Billet mis en vente	1
DOC_CLASS/RAR	Courrier recommandé	1
DOC_CLASS/REFUND_CREDIT_ACK	Remboursement	2
DOC_CLASSE/REQUÊTE CONFIRMATION	Courriel de confirmation	2
DOC_CLASS/REQUEST_CONTACT_CONSENT	Demande de consentement à la connexion de contact	1
DOC_CLASS/REQUEST_SUMMARY	Résumé de la demande	2

DOC_CLASS/RESET_OPERATOR_PASSWORD	Réinitialiser le mot de passe de l'opérateur	1
DOC_CLASS/RFD_PMT_NOTIFICATION_EMAIL	Courriel de notification de remboursement	2
DOC_CLASS/ST_SUBSCRIPTION	Abonnement à la carte d'abonnement ack/accusé de réception	2
DOC_CLASS/TAX_REFUND	Résumé du remboursement d'impôt	2
DOC_CLASS/TICKET_DETAILS_EMAIL	Détails des billets par courriel	2
DOC_CLASS/TICKET_RECEIPT	Reçu d'impression de ticket	2
DOC_CLASS/TICKETS_ACCUSÉ DE RÉCEPTION	Ticket ack/accusé de réception	2
DOC_CLASS/WAITACC_INVOICE	Facture en attente	10
DOC_CLASS/WAITACC_INVOICE_FINAL	Facture en attente (état final)	10