

# Data Protection Guide

Date	29 September 2022
Author	MKM / FLO / CPF
Reviewer	CPF / VLA
Version	2.6

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>2</b>
<b>2</b>	<b>Definitions.....</b>	<b>2</b>
<b>3</b>	<b>Regulatory requirements .....</b>	<b>3</b>
<b>4</b>	<b>S-360 features and characteristics.....</b>	<b>4</b>
4.1	Legitimate purposes and lawfulness of data processing .....	4
4.2	Fairness and transparency in data collection and processing .....	6
4.3	The relevance, adequacy and strict necessity of data .....	8
4.4	Use of cookies in the web interface or module .....	12
4.5	Data retention period.....	15
4.6	Accurate and up-to-date data. Rights of access, rectification, erasure and portability. Processing restriction and objection rights.....	16
4.7	Data security .....	19
4.8	Processors, sub-processors and cross-border transfers.....	21
4.9	Use of data for marketing purposes.....	21
4.10	Formalities.....	24
	<b>Appendix 1 Check list for completion by your organisation concerning Personal Data processing carried out using S-360 .....</b>	<b>25</b>
	<b>Appendix 2 List of SecuTix SA sub-processors .....</b>	<b>27</b>

## 1 Introduction

Since your organisation uses the S-360 platform provided by SecuTix SA, it acts as a Data Controller in that it collects and processes Personal Data concerning, in particular, customers who buy tickets, prospects, your own operators, and so on. Equally, SecuTix SA may act as a processor by transferring and/or processing this data to provide the solution as well as the services your organisation subscribes to.

When collecting, processing and transferring this Personal Data, you must comply with the applicable data protection regulations. As a Data Controller, you are solely responsible for compliance with the data protection requirements that apply to you.

In the European Union, the applicable regulations stem from European regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data. This is known as the General Data Protection Regulation (GDPR). It is directly applicable in all EU Member States from 25 May 2018.

SecuTix SA is subject to Swiss data protection legislation (see inset below). This legislation is very similar (identical in some cases) to the EU regulations. The European Commission has also decided (Commission decision 2000/518 CE of 26.07.2000), that Switzerland provides adequate protection for Personal Data transferred from the EU.

In addition, SecuTix SA will ensure that the solution it provides you with enables you to comply with European requirements in this area. This document, while non-exhaustive, outlines the relevant technical and organisational options included in S-360.

### Preliminaries

Firstly, we hereby state that:

- This data protection guide is purely intended to make you aware of the relevant S-360 features and the precautions we have taken to help you comply with certain legal or regulatory requirements that may apply to you as a Data Controller.
- This document is not a set of instructions for you to follow, nor does it constitute legal advice.
- The purposes for which you process data and the means you use to do so are your sole decision and sole responsibility. Consequently, you must send us your instructions using the check list in Appendix 1.

## 2 Definitions

**Personal Data:** Any information relating to an identified or identifiable natural person (referred to hereinafter as a 'Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (referred to in this document as 'Personal Data').

**Processing:** Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Data Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Where the purposes and means of such processing are determined by Union or Member State law, the Data Controller (referred to in this document as 'you' or 'your organisation') or the specific criteria for its nomination may be provided for by Union or Member State law.

**Data Processor:** A natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Data Controller (referred to in this document as 'we' or 'SecuTix SA').

**Data Subject:** A natural person whose Personal Data are subject to processing in S-360.

**Personal Data breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

### 3 Regulatory requirements

The European regulation requires all Data Controllers to comply with the following principles:

- Data shall be collected and processed lawfully, fairly and in a transparent manner.
- Data shall be processed for specified, explicit and legitimate purposes. Personal Data shall not be further processed in a manner that is incompatible with those purposes.
- The data collected and processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. They shall be accurate and kept up to date. Certain data of a sensitive nature shall only be collected and processed under certain conditions, in particular, with the Data Subject's consent.
- Data shall be kept for no longer than is strictly necessary for the purpose(s) for which they are processed.
- Data Subjects shall be informed that their Personal Data will be processed, and their consent shall be requested for certain types of processing. Certain information that must be given to such Data Subjects is mandatory.
- Data Subjects shall have a guaranteed right of access to and rectification or erasure of Personal Data, and the right to restrict or object to processing as well as the right to data portability. Data Subjects also have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.
- Data Controllers shall take appropriate technical and organisational measures to ensure data security, in particular, to prevent the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of data. (In some cases,

an impact assessment will be necessary in order to evaluate whether the planned measures are adequate. This may require the Data Controller to consult the relevant supervisory authority.) Personal Data breaches shall also be reported to the supervisory authority via a specific notification process, and in certain cases, to the Data Subjects affected.

- Data Controllers who use Data Processors and/or Sub-processors to process Personal Data shall do so under a specific contractual framework (cf. mandatory clauses).
- Cross-border flows of Personal Data to non-EU Member States that are not recognized as providing an adequate level of protection must be subject to sufficient and in particular, contractual, safeguards.
- Any organisation that collects and processes Personal Data shall establish and maintain:
  - records of Personal Data processing activities implemented under its responsibility as a Data Controller
  - records of Personal Data processing activities implemented under its responsibility as a Data Processor.

**Focus – data protection principles and commitments in Switzerland (Federal Data Protection Act):**

All data processing shall be lawful. All processing shall comply with the principles of good faith and proportionality. Personal Data shall only be processed for the purpose stated at the time of collection, or for the purpose provided for by law or by the circumstances. Data Subjects shall be made aware that their Personal Data are being collected and especially the purposes for which the data will be used. Where their consent is required in order to process their Personal Data, such consent is only valid if they give it freely and after having been properly informed. In addition, their consent to the processing of sensitive data and personality profiles shall be explicit. Personal Data shall be protected against unauthorised processing by appropriate organisational and technical measures.

## 4 S-360 features and characteristics

This paragraph (4) describes:

- the requirements and obligations that you must comply with as per paragraph 3 above
- the S-360 features and properties that enable you to do so.

### 4.1 Legitimate purposes and lawfulness of data processing

#### 4.1.1 Principles

The Data Controller is responsible for ensuring that:

- the data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (cf. purpose principle)
- the data are collected and processed lawfully in S-360 (cf. lawfulness principle).

Note that processing is lawful only if and to the extent that at least one of the following conditions applies:

- The Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

#### 4.1.2 S-360

The S-360 IT solution includes the following features:

- Ticketing management: configuration, planning, reservation, sales, issue, printing, access control, operator management, etc.
- Customer relationship management (customers and prospects): marketing campaigns, prospection and solicitation activities and the associated operations: selection, segmentation, data enhancement, targeting, email, analytics and tracking (website browsing and emails), and reports (statistics and performance).
- Event management: organisation, planning, speakers/guides, etc.
- Shop and sales management: stock/procurement/supplier management.

As a Data Controller, you have chosen S-360 as the system most suitable for processing Personal Data for purposes that you have determined and that are specific to your activities. It is your responsibility to ensure compliance with the above principles of purpose and lawfulness.

## 4.2 Fairness and transparency in data collection and processing

### 4.2.1 Principles

Data Controllers shall inform Data Subjects of the way in which their Personal Data will be processed (cf. fairness and transparency principle) in compliance with the applicable Personal Data protection provisions. In certain cases, they must also have given their consent (cf. paragraphs 3.1, 4.3 and 4.9 in particular).

In addition, all data collection forms shall include the relevant information.

### 4.2.2 S-360 and end customers

Therefore, as a Data Controller, you are responsible for informing Data Subjects as indicated above and for obtaining their consent where appropriate. Naturally, we are happy to provide you, on request, with any information we hold that would assist you in doing so.

In addition, to enable you to meet your obligations, we hereby inform you of the following:

- The S-360 web interface has a built-in 'Privacy Statement' tab. This can be accessed from every web page and has a hypertext link that redirects users to a page where you can add your own data protection statement or policy, which you are responsible for drafting:

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

- If you are using our web module integrated in your website, you should add a tab like this to your site.
- All online data collection forms in our web interface and web module (if integrated in your website) include an inset (which you are responsible for drafting and hosting) that allows you to add your statement, a checkbox to obtain consent, and a link to your privacy statement (which you are responsible for drafting and hosting). These two links need to be entered in the internet point of sale parameters.
- S-360 provides the Friends & Family feature allowing a contact (the lead of a group) to include members to his group and perform some operations on behalf of these members (buy tickets, pay reserved tickets, etc.). The lead of the group is also able to know the email address of the group's members. S-360 has implemented a new consent allowing the group lead to use the full extent of the Friends & Family feature only if the member has given his consent. This new behaviour is enabled by a parameter at organisation level:

Mandatory request consent for friend and family features  yes  no

We strongly advise you to enable this consent, Only customers already using the Friends & Family feature may keep the consent temporarily disabled in order to have some time to inform their internet users.

In addition, may we remind you that customers who make a reservation via offline channels must also be informed. Consequently, you are responsible for ensuring that your information process for every data collection method is compliant with the applicable data protection provisions (for example, in operators' scripts or on an interactive voice server for telephone sales, and on display at the box office).

In any case, you have an obligation to inform all Data Subjects (various contact types, operators, suppliers, prospects, etc. whose data may appear in S-360), and not just those who make a reservation. Equally, it is your responsibility to ensure this and to deploy the necessary processes.

### 4.2.3 S-360 and your operators

#### 4.2.3.1 Audit logs and operator actions

S-360 stores an audit log and a log of operator actions. Both logs are automatically deleted after 12 months.

The audit log stores the changes brought to the set-up and allows to find the previous state of the data. Such a log is mandatory in some countries for accounting purposes, for example to identify when a catalogue price has been changed.

The log of operator actions logs the actions performed by the operators. It may be used by our support team when an incident is raised in order to find back the exact sequence of operations.

#### 4.2.3.2 Posts about S-360 features

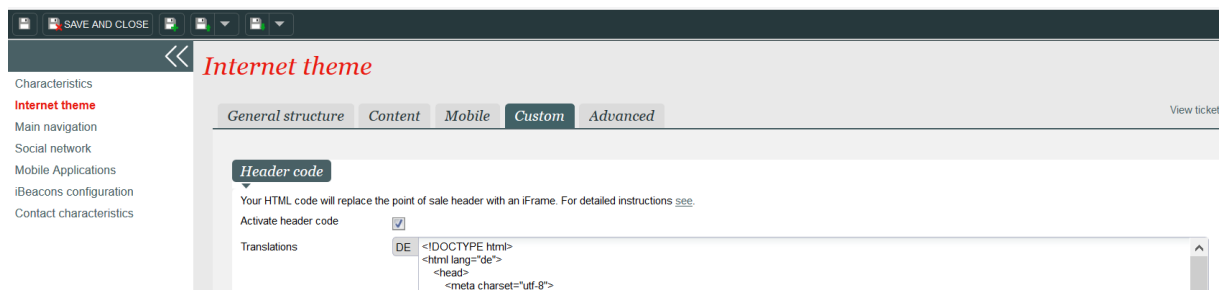
S-360 has recently integrated a new tool to the Release notes space of the Confluence web site, called GetBeamer. This tool allows us to send posts about our release notes or a specific feature.

The same tool will be integrated in the back-office module during the second half of 2022.

GetBeamer provides statistics about the reading of these posts. Since GetBeamer doesn't have access to the connection code or name of the operator, it identifies each operator with a fake name. As a result, these statistics are purely anonymous.

### 4.2.4 Customisation of S-360 Ticket Shop

The S-360 Ticket Shop may be customised in different ways. For example, the screen below allows to replace the standard header by your own HTML code:



The screenshot shows a web browser window with a dark header bar containing 'SAVE AND CLOSE' and navigation icons. Below the header, the page title is 'Internet theme'. A left sidebar lists configuration categories: Characteristics, Internet theme (selected), Main navigation, Social network, Mobile Applications, iBeacons configuration, and Contact characteristics. The main content area has tabs for 'General structure', 'Content', 'Mobile', 'Custom' (selected), and 'Advanced'. Under the 'Custom' tab, there is a 'Header code' section. It includes a text box with instructions: 'Your HTML code will replace the point of sale header with an iFrame. For detailed instructions see.' Below this is a checked checkbox for 'Activate header code' and a 'Translations' table. The table has a 'DE' entry with the following HTML code: 

```
<!DOCTYPE html>
<html lang="de">
<head>
<meta charset="utf-8">
```

HTML code may also be added directly, i. e. without using the S-360 back-end, through CSS.

You are solely responsible to keep GDPR compliance while customising our Ticket Shop by injecting some code, no matter the technic used. For example, according to a recent decision of a German court of justice, you should not use Google fonts by calling a Google service directly, because Google will store your end customer's IP address and keep it after having delivered the fonts. SecuTix provides the possibility to store Google fonts on its own servers in order to protect your end customer's privacy.

## **4.3 The relevance, adequacy and strict necessity of data**

### **4.3.1 Principles**

The data collected and processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (cf. data collection minimisation principle).

You may only collect and process the data that is required for the purpose (e. g. reservations, seat allocation or order payment). Since the regulations specify that it is strictly prohibited to collect data that is unrelated to the purpose of processing, Data Subjects must be able to choose whether or not to provide non-essential data.

There are also certain particularly sensitive data that must not be collected or processed. Indeed, as a matter of principle, collecting and processing the following data is prohibited

- So-called 'special categories' of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, plus genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
- Information relating to criminal convictions and offences or related security measures (such as a stadium ban).

There are exceptions to these prohibitions. For example, 'special categories' of data may be processed if they are necessary to processing and one of the following applies:

- The Data Subject has given their consent.
- Processing is being carried out by a foundation, an association or any other not-for-profit body with a political, philosophical, religious or trade union aim (under certain conditions).
- The Data Subject has manifestly made the data public.

Nonetheless, these exceptions must be interpreted strictly.

These principles apply regardless of the methods used to collect, capture and process the information in tools. Open comment fields, in particular, must be used with caution.

### **4.3.2 S-360**

As a Data Controller, you are responsible for ensuring compliance with the principle of data minimisation and the principle of prohibition on collecting certain data.



S-360 provides the option of default data collection fields, whether in the back office or in the web interface or web module. These fields are limited with a view to minimising data. At the same time, note that:

- These are default field options that you can change (apart from certain strictly mandatory fields for the solution to work properly, but these are very limited – for example, the only strictly mandatory data for contacts are salutation, last name and first name). As a Data Controller, you are responsible for determining which fields you use or add, in accordance with the information we request from you in Appendix 1 in order to instruct us in this respect.
- The same applies, for example, to the definition of ‘calculated’ data in the segmentation features, which you may choose to specify in Appendix 1.

In this respect, although S-360 gives you access to segmentation and possibly profiling features, you are the sole decision-maker (and therefore solely responsible) for the segments you wish to use, the purposes you are pursuing, the relevance, adequacy and necessity of the data processed in this context, the decisions you may have to make regarding these segments and the potential consequences for Data Subjects.

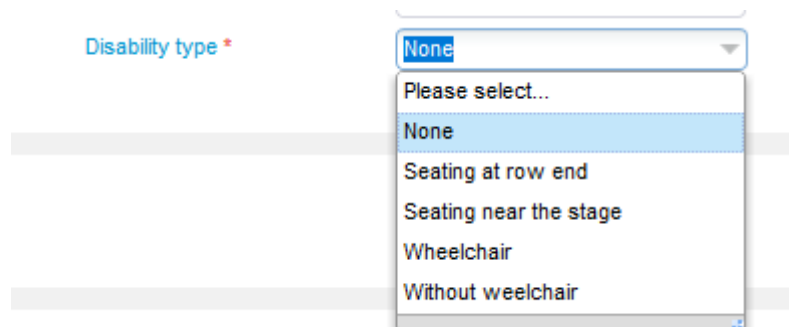
Also note that automated individual decision making by means of e.g. segmentation or, where applicable, profiling features may be subject to special precautions with which you are responsible for complying (consent, human intervention, the option to contest the decision, and so on).

- The same rules and principles apply to your choice and addition of reporting and retrieval criteria using the solution features. Moreover, given the data risks related to reports and retrievals once they are produced, we recommend that you set up an authorisation policy so that only those individuals with a strict interest are able to retrieve data (to be specified in Appendix 1).

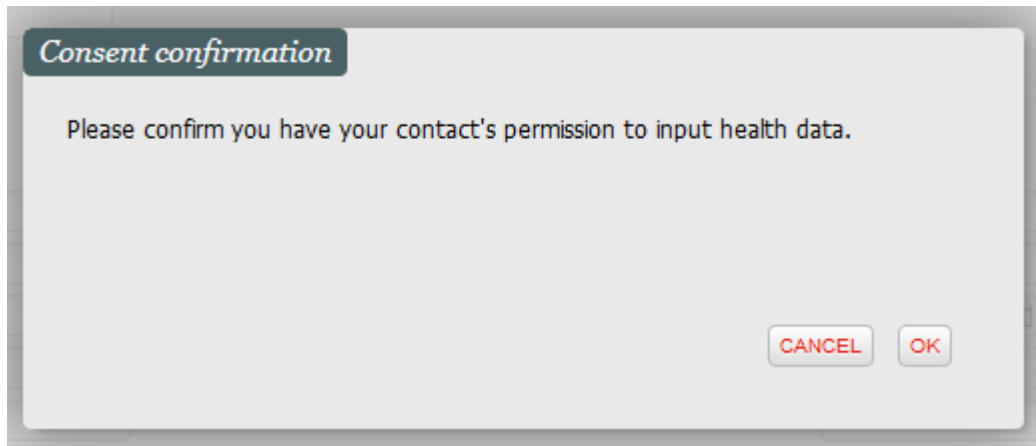
S-360 also has certain features designed to enable you to comply with the principles applicable to the data collected. For example:

- The default value for disability is ‘No disability’. In addition, this field is configured as a drop-down menu that restricts the operator’s options when entering the information. This is to limit the risk of collecting data that is not strictly necessary.

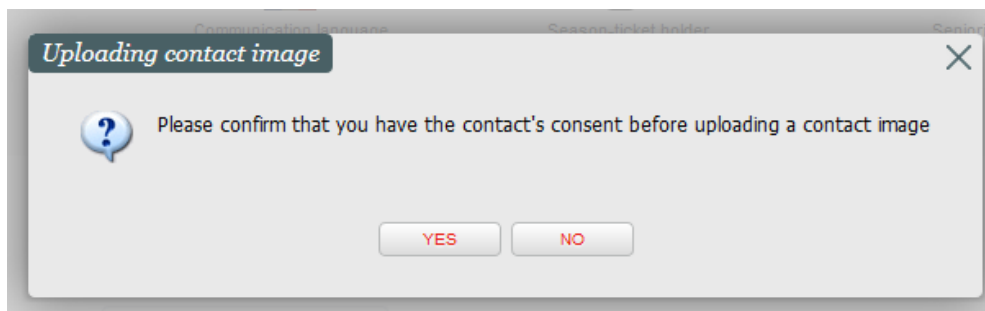
To enter another value, your organisation’s operator must confirm that they have asked for the contact’s consent, as follows:



The image shows a web form with a label 'Disability type \*' in blue text. Below the label is a dropdown menu. The dropdown menu is currently open, showing a list of options: 'None' (highlighted in blue), 'Please select...', 'Seating at row end', 'Seating near the stage', 'Wheelchair', and 'Without weelchair'. The dropdown menu has a small arrow icon on the right side of the top bar.



- To upload a photo, your organisation's operator must tick a box to confirm that they have requested the contact's consent, as follows:



If you authorize the contact to upload his photo on the web module, you have to add this consent into your online Privacy Statement.

- S-360 doesn't store a person's payment card data in plain text. Indeed, only a card alias is stored. S-360 may use this alias to perform later payments (example: payment by credit card in three times) but the alias doesn't allow to perform any other payment since it doesn't allow to find the credit card number. The Data Subject has to give his consent prior to the storage of the alias, whether:
  - by the Data Subject ticking a box in the interface or web module (not pre-ticked) or
  - by an operator ticking a box in the back-office (not pre-ticked and indicating that the contact's explicit consent is required).
- For open comment fields, your organisation's operator must tick a box during data entry to confirm that the comment complies with the applicable Personal Data protection provisions. In addition, operators can obtain more information by clicking a link, as follows:

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.

CLOSE

- For open comment fields of the web interface or web module shown on the finalization page of an order/reservation/option, it is your responsibility to set up the operator awareness and the processes necessary to moderate these comments. Furthermore, a simplified warning notice for contacts is inserted with the default text:

*“The data entered in this comment area should only be used to specify elements strictly necessary for the placing and/or execution of your order. In addition, we remind you that the information that you may communicate via this open comment field is subject to the provisions applicable to the protection of personal data, which you undertake to respect (lawful, objective, relevant, adequate and limited to what is necessary in relation to the purpose pursued, fairness of data collection and processing, etc.).”*

- The reporting and retrieval screens include a cautionary statement for S-360 users:

*‘When exporting this data you must ensure that you are acting in accordance with all applicable personal data protection principles. In particular, you must ensure that the resulting file will only be used as an extension of the initial processing and only for the same purposes as those pursued in the context of this application. You must also ensure that the data retrieved are relevant, adequate and strictly necessary for the purpose for which you intend to use it, and share it only with authorised people. It is your responsibility to take all necessary steps to ensure that the information is secure and, in particular, kept confidential. The export file must be stored for no longer than envisaged for data processed in the context of this application.’*

## 4.4 Use of cookies in the web interface or module

### 4.4.1 Principles

S-360 allows you to analyse online user behaviour with Google Analytics. Your organisation may use this feature, or may ask SecuTix SA to do so on its behalf, to improve your service. It measures visitor numbers as well as browsing and visit statistics.

Online users must be informed that you are using Google Analytics cookies, and their consent is required in order to track their visits.

To do this, a banner is displayed to online visitors who visit the website (homepage or subpage) This banner provides the following features:

- It describes briefly the different kinds of cookies and provides a link to a detailed but easy-to-understand explanation of the cookie categories and the cookies within each category
- It provides the choice between refusing all cookies (except the essential ones), accept all cookies or choose the cookie categories to accept

- The internet user cannot navigate further until he has chosen one of the options described above. In other words, the consent cannot be implicit

No cookie can be stored prior to user consent.

Finally, users who give their consent to you storing or reading cookies must be able to withdraw it at any time. In the event that Data Subjects give their consent, your site must request it again after 13 months in any case (cf. maximum lifetime of cookies).

For your information, there is a derogation from the requirement to obtain consent to visitor-number cookies provided that the following conditions are met:

- The user has been informed (cf. banner).
- The user has the option to object to the use of these cookies via a mechanism that is easy to use on any device, operating system, application or browser. You must not collect any information on people who choose to exercise their right of objection, or send it to the publisher of the visit frequency analysis tool.
- The purpose of the cookie must be limited to measuring how many people view the displayed content in order to evaluate both the content itself and the site or application ergonomics.
- Collected data must not be cross-checked against other processed data (e.g. customer files or visit frequency statistics from other sites). Use of the stored cookie must be strictly confined to producing anonymous statistics. Its scope must be limited to a single publisher and must not enable users to be tracked while using other applications or websites.
- Collected data can only be transferred to countries providing an adequate level of data protection
- If your organisation captures IP addresses for geotagging, the address must provide no information more detailed than the town or city. The IP address must also be deleted or anonymised after geolocation to prevent any other use of the data or any overlap with other personal information.
- Cookie lifetime must be limited to 13 months, and cannot be extended automatically during new visits. Data collected via cookies must be kept for no longer than 13 months.

For example, if you aren't 100% sure that the web analytics tool you want to use meets all these requirements, the use of it must be subject to a prior explicit consent.

#### **4.4.2 S-360**

As a website publisher (whether you use our web interface, or integrate our web module in your own website), you are responsible for informing online users about cookies and obtaining their consent to store and read them.

Where this is concerned:

- Upon request on SecuTix SA customer support tool, you can request whereby our interface and web module give you the option to display a cookie information banner and cookie consent dialogue when a user first visits the site. The wording of the information on this banner is your responsibility. For all practical purposes we suggest the following, which you can modify or adjust according to the specifics of your own website:

**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](#).

 Essential Audience measurement Customisation

You must implement this type of banner whether you use our web interface or have our web module integrated in your website. The banner must be configured to appear on whatever page of the site the user lands on, even if it is a subpage and not the homepage.

- You are responsible for drafting your cookie policy. The cookies we use in the context of our web interface are described in <https://confluence.secutix.com/display/DOCEN/List+of+cookies+used+on+this+site>.

You must include this information in your cookie policy.

You must implement this type of cookie policy whether you use our web interface, or our web module integrated in your website.

- As a matter of principle you should not place cookies unless the visitor provides his explicit consent (except for cookies that are essential to the processing of the order), and the banner must reappear 13 months after you first obtain their consent to your use of cookies. This is the default configuration setup by SecuTix SA after your service request. If you use our integrated module, you should ensure compliance with this obligation on your own website.
- If you wish to exempt your organisation from the obligation to obtain consent (in order to place cookies from the homepage), you should configure the cookies according to the principles above on visitor-number cookies that are not subject to consent. For example, if you're operating in France, you can find a list of web analytics tool exempt from consent on <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-dauidence>.

You must also comply with the other obligations required for exemption from consent.

Warning, this consent exception is only accepted for audience measure cookies: using different cookies such as social network cookies or advertising cookies require a preliminary user consent.

## 4.5 Data retention period

### 4.5.1 Principles

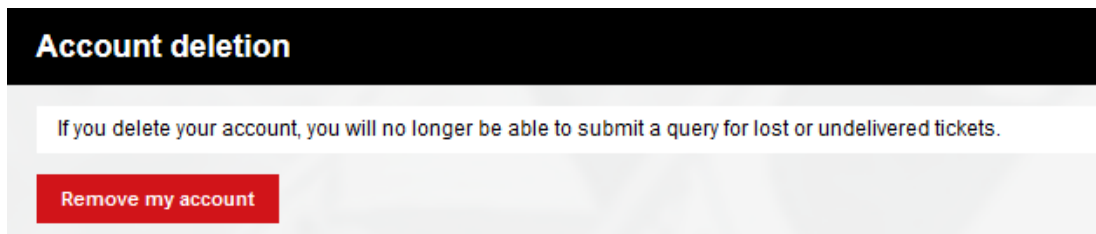
The Personal Data protection provisions require Data Controllers to retain data for no longer than is proportionate to its purposes. However, they give no indication of an exact retention period. Indefinite storage of Personal Data is not allowed under any circumstances.

### 4.5.2 S-360

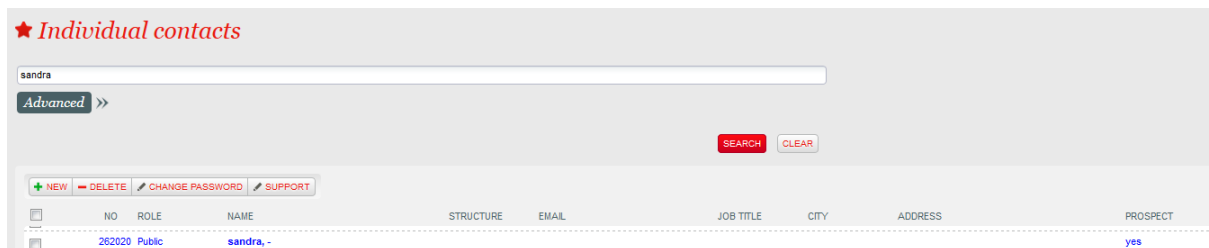
As a Data Controller, you are responsible for specifying and enforcing a maximum data retention period in the tools you use for processing Personal Data, in particular in S-360. This maximum applies to all Data Subjects whose data are collected and processed in S-360.

S-360 provides several data deletion features:

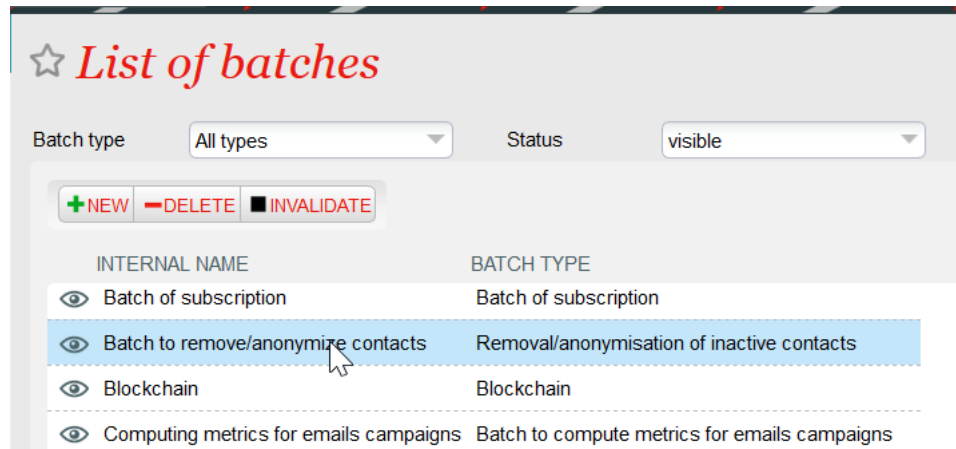
- Contacts with a personal online account can delete their data from this account:



- Operators in your organisation can delete contacts:



- In both cases, the contact's account and marketing information (history and indicators) are deleted and all orders anonymised. Data anonymisation becomes irreversible when the logs are deleted, i.e. after 12 months (cf. log retention period).
- Operators in your organisation can delete prospects.
- Your organisation's operators can manually anonymise the data of any Data Subject.
- S-360 also has a feature allowing you, according to your choices, your habits, your industry and related regulations, to detect contacts who have been inactive for more than  $n$  months and a batch deletes/anonymises them:



- After setting an operator's state to "suspended", you can anonymise the operator by simply replacing their last name, first name, email address, etc. with XXXX. Data anonymization becomes definitive when technical logs are deleted, ie after 12 months (cf log retention delay). Be aware that you cannot change/anonymise the login code of operators. Thus the administrators who create operators are responsible for ensuring they do not enter any information that allows the individual to be identified.

In any case, at the end of the contract your data will be retrieved and returned to you in the latest industry standard format. They are then removed from S-360 and are subject to the same purge rules as for manual deletion (cf. above).

## 4.6 Accurate and up-to-date data. Rights of access, rectification, erasure and portability. Processing restriction and objection rights.

### 4.6.1 Principles

Under the terms of the applicable Personal Data protection provisions, processed data shall be accurate and, where necessary, kept up to date. Data Controllers shall take appropriate steps to ensure that data inaccurate for the purposes for which they are processed are erased or rectified.

Data Subjects shall be guaranteed right of access to their data, the right to the portability of their data and the right to rectify and erase their data.

In addition, they have a right to restrict and/or object to the processing of their data.

These obligations are the responsibility of the Data Controller. However, the Data Processor shall assist the Data Controller in meeting its obligation to respond to requests from Data Subjects who wish to exercise their rights.

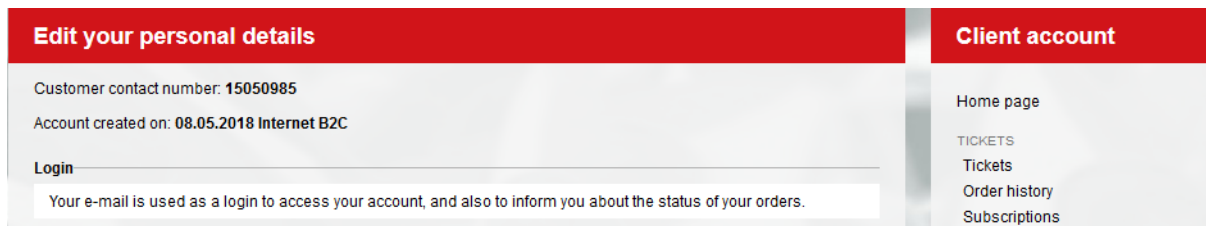


#### 4.6.2 S-360

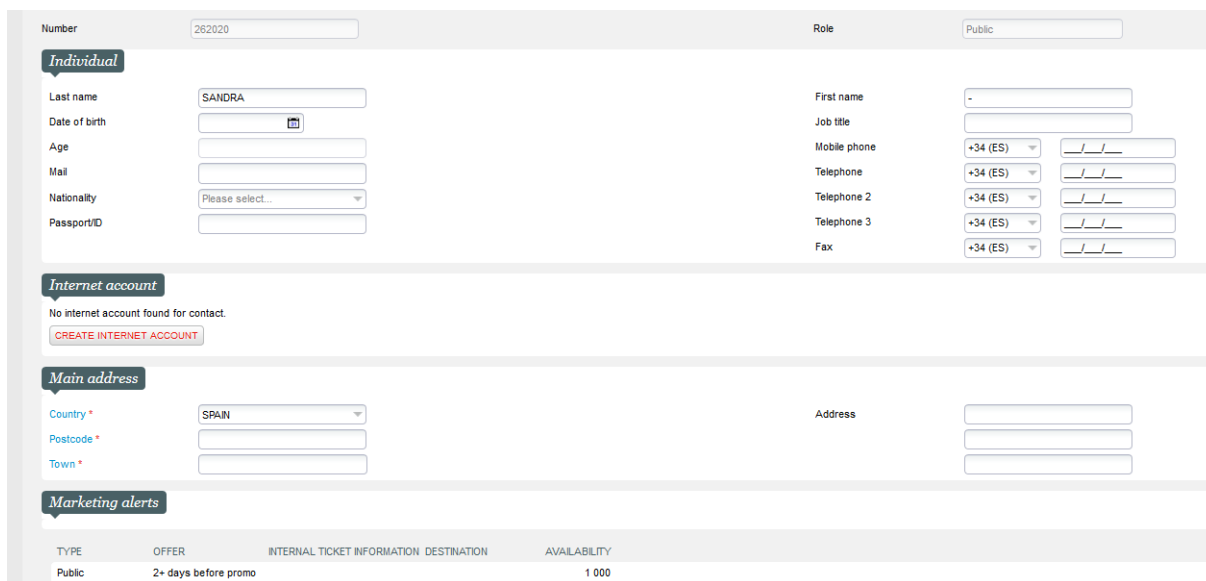
When Data Subjects exercise these rights, as a Data Controller you must ensure that you furnish them with the answers provided for by the applicable provisions and that their requests (provided they meet the requisite conditions) are followed up. Where this is concerned, note that we will tell you if a request is addressed to us directly, but responding and taking the required steps remain your sole responsibility.

S-360 includes features designed to manage rectification and erasure requests concerning data in the S-360 database.

- Users can change their profile data at any time in their personal online account:



- Your organisation's operators can update contact files:



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

- See paragraph 4.5 for information on data erasure requests.

When exercising their data access or portability rights, contacts may request all the personal information you hold on them. Your organisation's operators have access to contacts' data in order to respond to these requests. They can also obtain all the information stored on a contact (contact file, purchase history, relationship history) by submitting a request to SecuTix SA.

In addition:

- The source of information in the contact file is indicated. Possible values are:

- **IMPORT:** information collected via data import, for example data migration during the onboarding
- **BACKOFFICE:** information entered by an operator from your organisation outside the context of a booking or sale
- **Type of sales channel:** Information entered from a sales channel of the specified type. The mentioned type informs you whether the information has been entered by an end user (example: internet B2C sales channel), by an operator from your organisation (example: box office) or by an external operator (example: B2B2C sales channel)

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

Summary General Marketing Management Notes Administration

Created from	<input type="text" value="IMPORT"/>	Date inserted	<input type="text" value="25/07/2016"/>
User inserted	<input type="text" value="MPCTCT_SERV-240"/>	Date Updated	<input type="text" value="15/08/2017"/>
User Updated	<input type="text" value="STX-73980-pre"/>		

- The creation date of personal accounts is available from the account concerned:

**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.

- The contact file creation date and last modification date are indicated in the file:

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

Summary General Marketing Management Notes Administration

Created from	<input type="text" value="IMPORT"/>	Date inserted	<input type="text" value="25/07/2016"/>
User inserted	<input type="text" value="MPCTCT_SERV-240"/>	Date Updated	<input type="text" value="15/08/2017"/>
User Updated	<input type="text" value="STX-73980-pre"/>		

Ultimately, you are responsible for managing data processing restriction requests and objections.

In any case, we are committed to providing you with all the data elements we hold, on request, to enable to you to respond to Data Subjects who wish to exercise their rights, and we will make the necessary resources available.

## 4.7 Data security

### 4.7.1 Principles

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

You must therefore implement adequate security and confidentiality measures. For recommendations on data security, refer to: <https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>.

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data.

In the event of a Personal Data breach (a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to processed Personal Data), the Data Controller shall notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. When the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall notify the Data Subject without undue delay.

### 4.7.2 S-360

As a Data Controller, you are responsible for ensuring that you comply with all of these obligations.

As a Data Processor, SecuTix SA is responsible for deploying the appropriate security measures, notifying the Data Controller of any Personal Data breaches without undue delay after becoming aware of them, and more generally has an obligation to cooperate with the Data Controller in order for it to comply with its obligations (in particular, the deployment of appropriate security measures, and impact assessment).

SecuTix SA guarantees to meet the requirements of and obtain certificates of conformity to ISO/IEC 27001:2013 and PCI DSS v3.2. Thus, SecuTix SA undertakes to implement the technical and organisational security measures identified in these standards.

In addition, regarding S-360:

- Data are duplicated in real time on several redundant disks.
- Data are duplicated in near real time in two data centres several kilometres apart.
- To secure the servers and the solution appropriately, SecuTix SA takes all the necessary technical and organisational steps, in particular, access controls, the use of current firewalls and anti-virus programs, SSL encryption and logging when manually changing databases.
- The financial component of S-360 is PCI DSS certified and audited once a year.
- Passwords must have a number and a secure combination of characters and numbers to be valid.
- S-360 has a continuity plan for moving from one data centre to another.
- Physical access in data centres is strictly controlled by codes, tracking, alarms, badges and CCTV.
- Data sent to the backup site are encrypted via VPN or HTTPS.

In addition, in compliance with our obligations, we undertake to cooperate with you with a view to:

- enabling you to meet your own obligations regarding the security and, in particular, the confidentiality, of Personal Data.
- enabling you to carry out impact assessments on the processing of Personal Data if the nature of the processing we are involved in requires it, and to consult the supervisory authority where necessary regarding this processing
- meeting your obligation to notify the supervisory authority and inform the Data Subject in the event of a Personal Data breach. To this end, we will notify you of any Personal Data breaches of which we become aware. We also undertake to use all resources at our disposal and to inform you, at your request, of any documentation we hold that would be useful to you if you should need to submit these notifications.

You should also take the appropriate internal technical and organisational steps to ensure an appropriate level of security for data processed in S-360. For example, we recommend that you:

- safeguard and maintain current S-360 access (hardware, software, network, internet access)
- ensure that the passwords your organisation's operators use to connect to S-360 are confidential, and ensure that a password policy is put in place in compliance with applicable recommendations (cf. for illustrative purposes, see the recommendations available here: <https://www.cnil.fr/en/passwords-minimum-security-recommendations-businesses-and-citizens>). As a result, different operators of your organisation must never share the same S-360 login.
- keep antivirus programs up to date on all workstations
- etc.

## **4.8 Processors, sub-processors and cross-border transfers**

### **4.8.1 Principles**

Data Controllers who use Data Processors and/or Sub-processors to process Personal Data shall do so under a specific contractual framework that includes certain mandatory clauses.

Cross-border flows of Personal Data to non-EU/EEA Member States and/or not recognized by the EU Commission as providing an adequate level of protection shall be only be implemented if they are subject to sufficient and, in particular, contractual, safeguards.

### **4.8.2 S-360**

As part of S-360 service provision, we need to process Personal Data on your organisation's behalf, which means we would be acting as your Data Processor. The contractual documents that we provide for this purpose include a clause outlining our services in this role as Data Processor, in compliance with GDPR requirements.

Given that we supply the solution, various entities in our group need to process Personal Data on your behalf. In this regard, note that our group entities are mainly based in the European Union or in Switzerland, providing an adequate level of data protection. However, one entity is based in Vietnam. In compliance with the applicable data protection provisions, cross-border data-flows to this entity are governed by the ELCA Standard Contractual Clauses agreement based on the models established by the EU Commission revised according to guidance from the Swiss Federal Data Protection and Information Commissioner (FDPIC).

In addition, depending on the services included in your subscription, in order to provide you with all the features offered as part of S-360 we need to use additional Sub-processors. These are listed in Appendix 2.

## **4.9 Use of data for marketing purposes**

### **4.9.1 Principles**

With regard to the use of data for marketing purposes, the following principles apply:

- Data Subjects shall give their express consent (opt-in via an empty tick box accompanied by wording inviting the Data Subject to opt in) to receive email, sms, mms, fax and automated electronic communications (cf. automated calls).
- Data Subjects shall not have previously opted out of postal mail communication or phone contact with human intervention.
- Every communication sent (in particular, email and sms) shall include a simple, free way to unsubscribe (right of objection) from communications via the channel concerned, and the subject line of emails shall relate to the email content and specify on whose behalf it is being sent.

With regard to email, sms or mms, note that an exemption from the requirement for consent may be exercised provided that all the following conditions are met:

- The recipient's contact details were collected during a sale or when providing a service.
- The communication complies with applicable Personal Data protection provisions, in particular as regards information on individuals.
- Direct prospecting concerns similar products or services provided by the same natural or legal person.
- Addressees shall expressly and clearly be given the opportunity to object easily and at no cost (except for charges related to sending the objection) to the use of their contact details at the time when these are collected and each time the contact receives a prospecting email.

#### 4.9.2 S-360

S-360 includes marketing features that enable you to send promotional messages to your contacts (customers and prospects). However, how you use these features is your sole responsibility and you must comply with the above principles.

To enable you to carry out your marketing activities in compliance with these principles, SecuTix SA has put in place the following features:

- The form provided for online visitors to create an online personal account via our interface or web module includes an insert for the statement that you are responsible for drafting. You must fill out the statement using empty tick boxes and the required wording informing users that their consent is required/that they may object to the use of their data. These items should be entered in the internet point of sale parameters.
- Online users have several default features in their personal online account, as follows:
  - Subscribe/unsubscribe to/from newsletter(s) (adaptable to your needs):

I would like to subscribe to the newsletter	<input type="radio"/> Yes	<input type="radio"/> No
---	---------------------------	--------------------------

- A choice of communication channels and senders (adaptable to your needs):

	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"/>

- At the box office (in the back office):
  - Your organisation's operators can specify whether a contact is happy to receive communications from your organisation, partners of your organisation, and third parties

*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

- Your operators can specify which communication channels the contact prefers:

*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"/>

- All boxes are empty by default. Equally, opt-in requires positive action by the online visitor or an operator. You should take these management rules into account in order to carry out your marketing activities in compliance with the principles in paragraph 4.9.1.

You should also take account of requests objecting to prospection that are brought to your attention by Data Subjects (by ticking 'no' for the communication channels in question).

To summarise, you must take into account the following principles:

- You must not prospect a contact via a communication channel marked "no".
- You may only prospect by email, sms, mms, fax or automated electronic communications systems via a communication channel marked "yes"
- You may prospect by post or carry out telemarketing via a communication channel marked "yes" or left empty (cf. neither "yes" nor "no").'

Newsletters that S-360 sends at your request contain, as a minimum, information allowing recipients to exercise their right of objection (i.e. that they wish to receive no more communications of this kind). These communications include an unsubscribe link. Unsubscription is automatically taken into account in S-360 (the system sets the box to 'no'):

© Museum of Science and Art, all rights reserved

62, rue de Lille, 75007 Paris

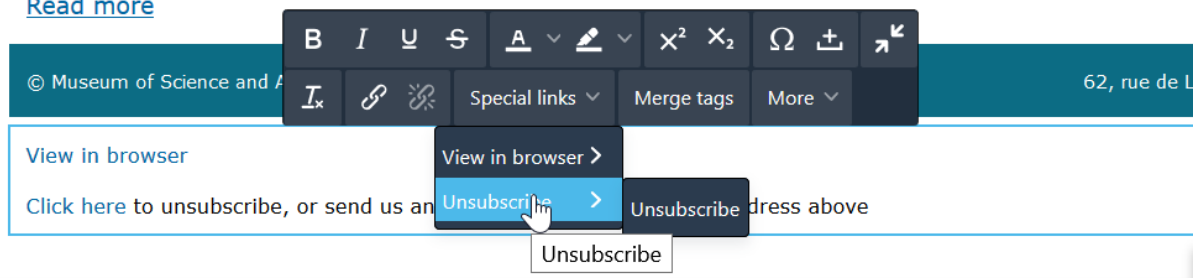
[View in browser](#)

[Click here](#) to unsubscribe, or send us an unsubscribe request to the address above

To include this feature in the emails that you send, please include one of the two solutions below in their configuration:

- Your organisation's operator configures the 'Unsubscribe URL' link. Contacts are automatically unsubscribed when they click on the link:

[Read more](#)



- Your organisation's operator adds a link redirecting contacts to their personal space, where they can opt out of their subscription or modify their preferences.

## 4.10 Formalities

### 4.10.1 Principles

Data Controllers shall maintain a record of processing activities under their responsibility.

Data Processors shall maintain a record of all categories of processing activities carried out on behalf of Data Controllers.

These records shall be in writing, including in electronic form. The Data Controller or Data Processor shall make the record available to the supervisory authority upon request.

### 4.10.2 S-360

As a Data Controller, you must integrate Personal Data processing implemented using S-360 into your 'Data Controller' processing activities record.

We as a Data Processor must integrate Personal Data processing implemented using S-360 on your behalf into our 'Data Processor' processing activities record.



## Appendix 1 Check list for completion by your organisation concerning Personal Data processing carried out using S-360

Question	Answer	remarks
Purposes for which your organisation uses the solution and the services included in your subscription		Objectives pursued, application functionalities chosen, actual or planned uses, purposes responding to specific provisions, consequences of the processing,...
Data collected and processed in the solution	...	Details of the data the customer wishes to collect and process when using S-360
Persons authorised to add new fields + method used to request this from SecuTix SA		Communicate the identity of authorized persons at the customer + specify how requests can be made to SecuTix SA
Persons authorised to add new segmentation criteria + method used to request this from SecuTix SA		Communicate the identity of authorized persons at the customer + specify how requests can be made to SecuTix SA
Persons authorised to add new reporting/retrieval criteria + method used to request this from SecuTix SA		Communicate the identity of authorized persons at the customer + specify how requests can be made to SecuTix SA
Recipients of "administrator" logins		It is then the responsibility of the client to determine and configure himself the persons who can have access to the data, as well as the details of the authorizations to the data, screens, functionalities (ex: consultation, input, reporting / extraction,...).
Desired data retention time in the solution		S-360 allows to define the data retention life span that then gives the customer the means to set the desired duration themselves.
Organisational contact in the event that Data Subjects wish to exercise their rights		Communicate the identity and contact information of the client
Organisational contact in the event of a data breach		Communicate the identity and contact information of the client

---

Data protection reference person

Communicate the identity and contact details of the Data Protection Officer of the customer, or at least the "Personal Data protection" referent

Further instructions from the organization to SecuTix SA

Specify any other instructions of the customer to the attention of SecuTix SA

## **Appendix 2 List of SecuTix SA sub-processors**

The list of SecuTix SA sub-processors is available [here](#).