

# Data Protection Manual

Date	12 November 2018
Author	MKM / FLO / CPF
Reviewer	CPF / VLA
Version	2.4

## 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>SecuTix 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 .....	5
4.3	The relevance, adequacy and strict necessity of data .....	6
4.4	Use of cookies in the web interface or module .....	11
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 .....	18
4.8	Processors, sub-processors and cross-border transfers .....	20
4.9	Use of data for marketing purposes .....	21
4.10	Formalities .....	23
	<b>Appendix 1 Check list for completion by your organisation concerning personal data processing carried out using SecuTix 360° .....</b>	<b>25</b>
	<b>Appendix 2 List of SecuTix SA sub-processors .....</b>	<b>27</b>

## 1 Introduction

Since your organisation uses SecuTix 360°, 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 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 SecuTix 360°.

### Preliminaries

Firstly, we hereby state that:

- This data protection manual is purely intended to make you aware of the relevant SecuTix 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 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.

**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 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.

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

**Data subject:** A natural person whose personal data are subject to processing in SecuTix 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 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.
- 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 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.

- Controllers who use 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 controller
  - records of personal data processing activities implemented under its responsibility as a 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 SecuTix 360° features and characteristics

This paragraph (4) describes:

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

### 4.1 Legitimate purposes and lawfulness of data processing

#### 4.1.1 Principles

The 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 SecuTix 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 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 controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the 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 SecuTix 360°**

The SecuTix 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 controller, you have chosen SecuTix 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**

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 SecuTix 360°

Therefore, as a 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 SecuTix 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:

[© 2018 SECUTIX](#) | [CREATED BY SECUTIX](#) | [GENERAL TERMS & CONDITIONS](#) | [PRIVACY POLICY](#) | [FAQ](#)

- 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.

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 SecuTix 360°), and not just those who make a reservation. Equally, it is your responsibility to ensure this and to deploy the necessary processes.

### 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 SecuTix 360°

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

SecuTix 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 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 SecuTix 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).

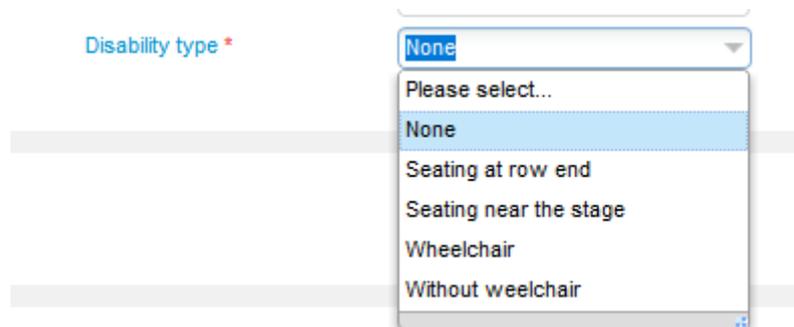
- The same rules and principles apply to your choice and addition of reporting and retrieval criteria using the solution features. Moreover, given the data risks related

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).

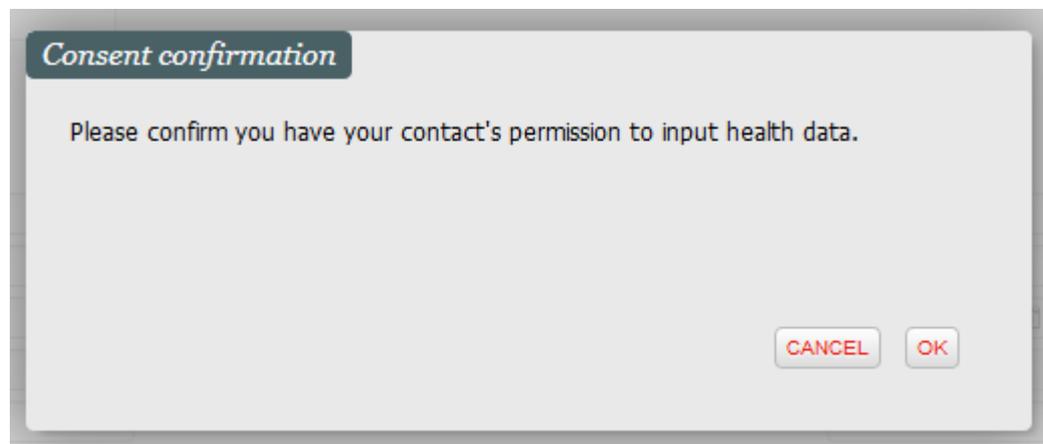
SecuTix 360° also has certain features designed to enable you to comply with the principles applicable to the data collected. For example:

- 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:

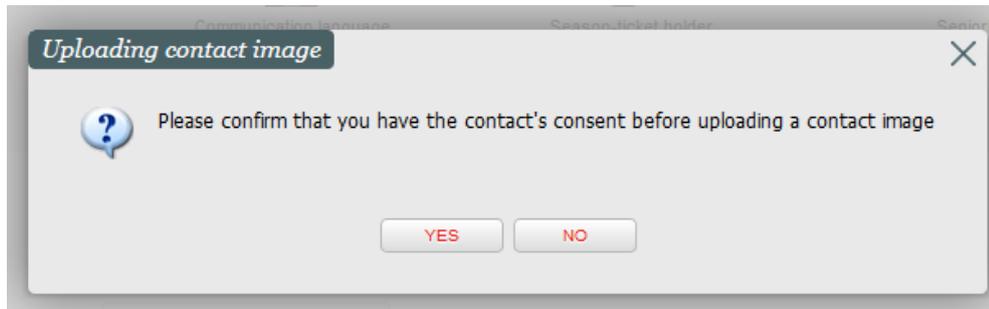


The image shows a form field labeled "Disability type" with a red asterisk. A drop-down menu is open, displaying the following options: "None" (highlighted), "Please select...", "Seating at row end", "Seating near the stage", "Wheelchair", and "Without weelchair".



The image shows a dialog box titled "Consent confirmation". The text inside reads: "Please confirm you have your contact's permission to input health data." At the bottom right, there are two buttons: "CANCEL" and "OK".

- 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.

- In SecuTix 360°, operators cannot see a person's payment card data in plain text. However, the data can be encrypted and securely saved when a contact makes a purchase as long as the data subject consents, for example to save their payment data for subsequent purchases (excluding the CVV/security number). By default, the save credit card information feature is disabled. Activating this feature requires the data subject's consent, 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:



*Note > New*

**Note**

Subject \*

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 SecuTix users:

*‘When exporting this data you must ensure that you are acting in accordance with the 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 them, and share them with authorised persons only. It is your responsibility to take all necessary steps to ensure that the information is secure and, in particular, 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

SecuTix 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, online visitors who visit the website (homepage or subpage) must be informed of the following via a banner that appears on the screen:

- the exact purposes of the cookies used
- the option to refuse cookies and to change user settings by clicking on a link in the banner (redirecting users to a cookies policy that provides them with a simple, easy-to-understand explanation of how to accept or refuse all or some cookies)

- that by continuing to browse the site they are agreeing cookies being stored on their computer.

Since consent has to be unambiguous, the banner must remain on the screen until the user continues browsing, i.e. until they visit another page or click on a site element (e.g. an image, link, or Search button).

This means that without the user's prior consent, you must not store and read cookies that are subject to consent:

- if users visit the site and do not continue browsing: simply taking no action does not constitute consent
- If they click on the link in the banner and, where applicable, refuse cookies by changing their settings.

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.
- 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.

#### 4.4.2 SecuTix 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 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:

By continuing to browse this site, you accept the use of cookies or similar technologies whose purpose is to produce statistics on visits to our site (visitor numbers, visit frequency, page views and performance tests and measurements), but also **[to be completed with other purposes if necessary, based on your web interface]**.  
 For more information and to set your preferences on cookies and similar technologies, click here [insert a link to your cookie policy].

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. However, note that the cookies we use in the context of your web interface are as follows:

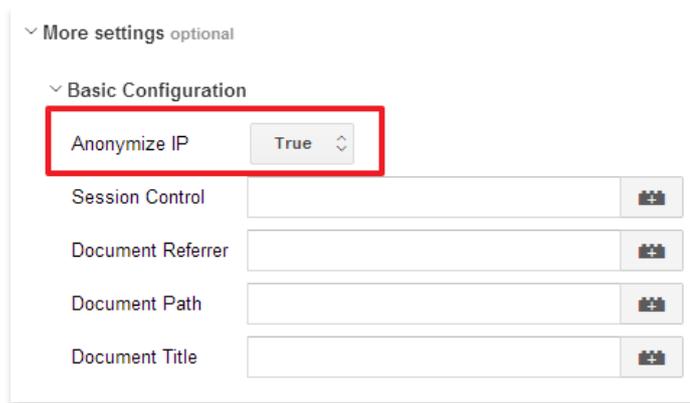
Type	Name	Publisher	Purposes	Lifetime
<b>Permanent ('persistent') cookie for statistics and for tracking visitor numbers and visit frequency.</b>	_ga	Google Inc. (Google Analytics)	<p>When Google Analytics is activated, these cookies are implemented based on information collected while users are browsing, in particular, their IP address, internet service provider and browser type, configuration and settings, etc.</p> <p>These cookies are used to distinguish individual site visitors to a site by assigning a randomly generated number as a user identifier. The identifier is updated with every page view and allows you to calculate, in particular, visitor numbers, session numbers and so on.</p> <p>For more information, see:  <a href="https://support.google.com/analytics/answer/6004245">https://support.google.com/analytics/answer/6004245</a></p> <p>Google Analytics deactivation module:  <a href="https://support.google.com/analytics/answer/181881?hl=fr&amp;ref_topic=2919631">https://support.google.com/analytics/answer/181881?hl=fr&amp;ref_topic=2919631</a>.            or  <a href="https://tools.google.com/dlpage/gaoptout">https://tools.google.com/dlpage/gaoptout</a>.</p>	?
<b>Session cookie</b>	lang		Allows to remember the user's language setting.	

<b>Session cookie for technical purposes</b>	SESSION		Session technical identifier.	
<b>Session cookie for technical purposes</b>	BIGipServer_XXX		Allows to route the contact to the same server in order to use caching options.	
<b>Technical session cookie</b>	AcpAT_XXX		Allows to verify that the contact has been routed via PeakProtect (peak traffic management tool)	

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 continues browsing, 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. In particular (but not exclusively), an operator in your organisation should configure Google Analytics to anonymise IP addresses before sending data to Google in the US so that no personal overlap is possible.



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

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

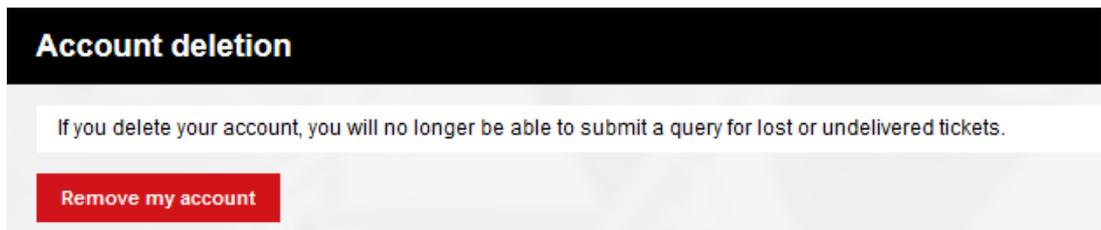
The personal data protection provisions require controllers to retain data for no longer than is proportionate to its purposes. However, they give no indication of an exact retention period. Indefinite storage of personal data is not allowed under any circumstances.

### 4.5.2 SecuTix 360°

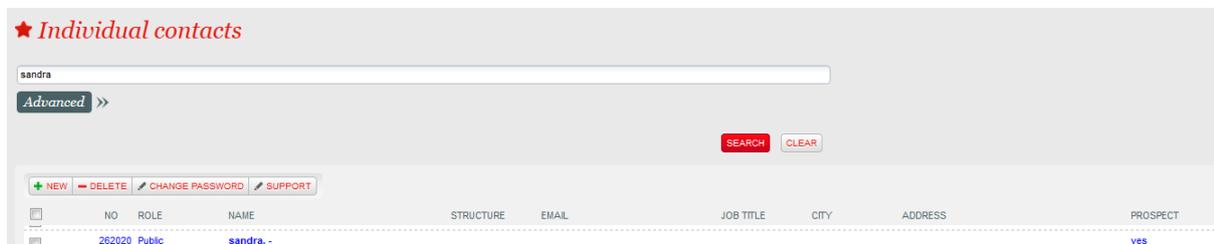
As a controller, you are responsible for specifying and enforcing a maximum data retention period in the tools you use for processing personal data, in particular in SecuTix 360°. This maximum applies to all subjects whose data are collected and processed in SecuTix 360°.

SecuTix 360° provides several data deletion features:

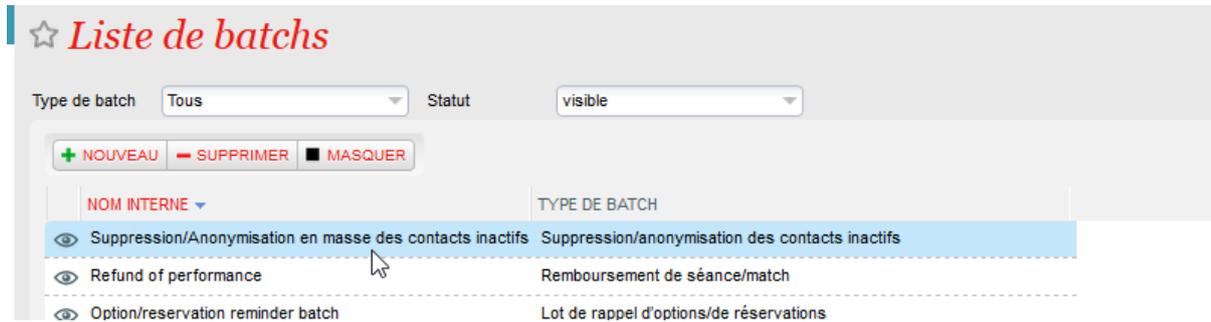
- Contacts with a personal online account can delete their data from this account:



- 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.
- SecuTix 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 SecuTix 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. 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 controller. However, the processor shall assist the controller in meeting its obligation to respond to requests from data subjects who wish to exercise their rights.

### 4.6.2 SecuTix 360°

When data subjects exercise these rights, as a 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.

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

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

Edit your personal details	Client account
<p>Customer contact number: <b>15050985</b></p> <p>Account created on: <b>08.05.2018 Internet B2C</b></p> <p><b>Login</b></p> <p>Your e-mail is used as a login to access your account, and also to inform you about the status of your orders.</p>	<p>Home page</p> <p>TICKETS</p> <p>Tickets</p> <p>Order history</p> <p>Subscriptions</p>

- Your organisation's operators can update contact files:

Number	262020	Role	Public
<b>Individual</b>			
Last name	SANDRA	First name	-
Date of birth	<input type="text"/>	Job title	<input type="text"/>
Age	<input type="text"/>	Mobile phone	+34 (ES) <input type="text"/>
Mail	<input type="text"/>	Telephone	+34 (ES) <input type="text"/>
Nationality	Please select...	Telephone 2	+34 (ES) <input type="text"/>
Passport/ID	<input type="text"/>	Telephone 3	+34 (ES) <input type="text"/>
		Fax	+34 (ES) <input type="text"/>
<b>Internet account</b>			
No internet account found for contact.			
<a href="#">CREATE INTERNET ACCOUNT</a>			
<b>Main address</b>			
Country *	SPAIN	Address	<input type="text"/>
Postcode *	<input type="text"/>		<input type="text"/>
Town *	<input type="text"/>		<input type="text"/>
<b>Marketing alerts</b>			
TYPE	OFFER	INTERNAL TICKET INFORMATION	DESTINATION
Public	2+ days before promo		AVAILABILITY
			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 as 'information entered by user', 'information entered by an operator from your organisation', or 'information collected via data import':

☆ *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				

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

### Edit your personal details

Customer contact number: 15050985

Account created on: 08.05.2018 Internet B2C

#### 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	IMPORT	Date inserted	25/07/2016
User inserted	MPCTCT_SERV-240	Date Updated	15/08/2017
User Updated	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 controller and 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 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 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 controller shall notify the data subject without undue delay.

#### **4.7.2 SecuTix 360°**

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

As a processor, SecuTix SA is responsible for deploying the appropriate security measures, notifying the controller of any personal data breaches without undue delay after becoming aware of them, and more generally has an obligation to cooperate with the 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 SecuTix 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 SecuTix 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.
- SecuTix 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 SecuTix 360°. For example, we recommend that you:

- safeguard and maintain current SecuTix 360° access (hardware, software, network, internet access)
- ensure that the passwords your organisation's operators use to connect to SecuTix 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>).
- keep antivirus programs up to date on all workstations
- etc.

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

### 4.8.1 Principles

Controllers who use 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 Member States that are not recognised 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 SecuTix 360°

As part of SecuTix 360° service provision, we may have cause to process personal data on your organisation's behalf, which means we would be acting as your processor. The contractual documents that we provide for this purpose include a clause outlining our services in this role as processor, in compliance with GDPR requirements.

Given that we supply the solution, various entities in our group may also have cause 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 a cross-border flow agreement based on the Swiss models put forward by the Swiss Federal Data Protection and Information Commissioner (FDPIC) and European models established by the European Commission.

In addition, depending on the services included in your subscription, in order to provide you with all the features offered as part of SecuTix 360° we may have cause to use 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 email communications 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 SecuTix 360°**

SecuTix 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  Yes  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  yes  no

Accepts transmission of elec. coordinates to third parties  yes  no

Accept communication from one partner  yes  no

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

**Communication**

Canal de communication préféré

SMS\_MMS  yes  no

Telephone  yes  no

E-Mail  yes  no

Letter  yes  no

Bounce status

- 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 raise user awareness, SecuTix 360° includes a warning notice on the screens allowing prospection activities, worded as follows:

*'As part of the prospection activities that you wish to carry out, note that 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 SecuTix 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 SecuTix 360° (the system sets the box to 'no'):

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

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:

Unsubscribe URL <https://citm-daysoff.shop.secutix.com/api/1/redirect/unsubscribe?id=xEiA2Zzp1h7SfXnCB%2FV9yP1qDbw%3D>

- 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

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

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

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

#### **4.10.2 SecuTix 360°**

As a controller, you must integrate personal data processing implemented using SecuTix 360° into your 'controller' processing activities record.

We as a processor must integrate personal data processing implemented using SecuTix 360° on your behalf into our 'processor' processing activities record.

## Appendix 1 Check list for completion by your organisation concerning personal data processing carried out using SecuTix 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 the SecuTix 360° solution
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		The SecuTix 360° solution 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

### Appendix 2.1 Sub-processors having access to end customer personal data

The table below lists all partners having access to end customer personal data. Sub-processors receiving a personal identifier (e.g. IP address) are also mentioned in this list regardless if additional personal data is sent or not. SecuTix subsidiaries, ELCA subsidiaries and other contractors performing sales (of SecuTix product), onboarding and customer supports may be involved at any time depending on institution's location. Technical partners are only involved if the institution has requested the feature provided by that partner. The only exception is our EFSTA partner which service is required to be compliant with fiscal laws of some countries (France and Austria).

Type	Name	Country	Activity	Type of data transfer	Data description	Processing description	Agreement with subcontractor
<b>SecuTix and subsidiaries</b>	<b>SecuTix SA</b>	France	Distributor and customer support	Access granted to database	All end customer data stored in SecuTix	Customer support and onboarding	No
	<b>SecuTix Iberia S.L.</b>	Spain					
	<b>SecuTix Ltd</b>	UK					
<b>ELCA and subsidiaries (except SecuTix)</b>	<b>Elca Informatique SA</b>	Switzerland	Software development, new customer onboarding, customer support, operation and maintenance, hosting	Access granted to database	All end customer data stored in SecuTix	Customer support and onboarding	No
	<b>Elca Spain</b>	Spain	Software development and integration, customer support				No
	<b>Elca Information Technology Ltd</b>	Vietnam	Software development, new customer onboarding, customer support, operation and maintenance				Cross border data flow agreement
<b>Other contractors for commercial and technical support</b>	<b>Nazaries</b>	Spain	Customer support	Access granted to database	All end customer data stored in SecuTix	Customer support and onboarding	No
	<b>Agorasophia Edutainment Spa Management</b>	Italy	Sales and onboarding				No
	<b>Swantegy USA LLC</b>	USA	Sales and onboarding				In progress

Type	Name	Country	Activity	Type of data transfer	Data description	Processing description	Agreement with subcontractor
	<b>Eric David (independent consultant)</b>	Switzerland	Customer support				No
<b>Full service providers</b>	<b>Orange Application For Business</b>	France	Sales and onboarding	Access granted to database	Only data of end customers of institutions under contract with mentioned provider	Customer support and onboarding	Contract (full service provider is a SecuTix customer)
	<b>Experient</b>	USA	Sales and onboarding	Access granted to database	Only data of end customers of institutions under contract with mentioned provider	Customer support and onboarding	Contract (full service provider is a SecuTix customer)
<b>Technical partners – Payment</b>	<b>Ingenico ePayment</b>	France/Belgium	Payment service provider	Data transferred	first name, last name, postal and email address	Authorise and execute payments. Personal data are foreseen for fraud detection	Direct contract between institution and partner
	<b>Paypal</b>	France/UK/Germany			email address	Simplify login to Paypal account	
	<b>Sharegrop</b>	France			email address	Manage payment of a given order by multiple persons	
	<b>Premium Credit</b>	UK			first name, last name, birth date, postal and email address, phone number	Data required to grant a loan	
	<b>Slimpay</b>	France			Bank account information	Data required to perform direct debit	
	<b>OnPaie</b>	France			Customer address data	Fraud detection	

Type	Name	Country	Activity	Type of data transfer	Data description	Processing description	Agreement with subcontractor
Technical partners – Other	Maxmind	USA	IP address geolocation	Data transferred	IP address No information on address holder	Find the related country, city and postal code	EU-U.S. & SWISS-US PRIVACY SHIELD
	EFSTA	Austria	Tax receipts	Data transferred	Purchaser name and address in encrypted form	EFSTA stores invoices with digital signature to ensure compliance with French regulations (NF525). EFSTA cannot decrypt data on its own initiative	No
	Orange Business Services – Contact Everyone	France	SMS routing	Data transferred	Mobile phone number (no information on number owner)	Send marketing campaigns through SMS	No
	DocuSign	UK	Digital signature of documents	Data transferred	First name and last name, email	Embed these information in digital signature	No
	Common Cents	France	Donation management	Data transferred	First name and last name, address, email	Provides donation certificate to end customers having performed a donation	No
	JMM Loyds	UK	Insurance company	Data transferred	First name and last name, order information	Ticket cancellation requests are directly handled by Loyds that needs to know the insured customers	Direct contract between institution and partner
	Fortress	UK	Access control solutions	Data transferred	Ticket information +	Check that a ticket is valid and that	Institution is already in

Type	Name	Country	Activity	Type of data transfer	Data description	Processing description	Agreement with subcontractor
					ticket holder information	ticket owner matches the person who tries to enter the venue	contract with Fortress
	<b>IdMobile</b>	Switzerland	Buy and pay tickets through mobile phone	Data transferred	Mobile phone number	End customer pays the ticket through his phone bill	Direct contract between institution and partner
	<b>MS Dynamics CRM</b>	US	Customer relationship management	Data transferred	All contact data	Institution benefits from MS CRM features to manage end customers	Direct contract between institution and partner
	<b>Optionizr</b>	France	Manage options	Data transferred	First name and last name, email, order data	Stores an option (e.g. for an event) and recalls end customer if he hasn't confirmed it after some deadline	No
	<b>Rewards4Group</b>	France/UK	Management of loyalty program	Data transferred	All contact data and matching sales data	Data are used to compute the number of loyalty points, convert them to a credit note and manage the number of used loyalty points	Data are only sent to the partner if the institution provides a loyalty program and the end user has subscribed to it.
	<b>Salesforce</b>	US	Customer relationship management	Data transferred	All contact data	Institution benefits from Salesforce features to manage end customers	Direct contract between institution and partner
	<b>Scotcomms</b>	UK	Access control solutions	Data transferred	Ticket information +	Check that a ticket is valid and that	Institution is already in

Type	Name	Country	Activity	Type of data transfer	Data description	Processing description	Agreement with subcontractor
					ticket holder information	ticket owner matches the person who tries to enter the venue	contract with Scotcomms
	<b>Skidata</b>	Austria	Access control solutions	Data transferred	Ticket information + ticket holder information	Check that a ticket is valid and that ticket owner matches the person who tries to enter the venue	Institution is already in contract with Skidata
	<b>Sports Alliance</b>	UK	Manage marketing campaigns for club fans	Data transferred	Contact, sales and access control data	Data are used to target marketing campaigns to a given group of end customers	Direct contract between institution and partner
	<b>Swisspass</b>	Switzerland	Single access card for transportation services and leisure	Data transferred	First name and last name, birthdate, address, tickets loaded on card	Load tickets on card, check tickets loaded on card	Direct contract between institution and partner. Switzerland only
	<b>Two Circles</b>	UK	Business intelligence in sports industry	Data transferred	Contact, sales and access control data	Data are used to generate reports and target marketing campaigns to a given group of end customers	
	<b>VE Interactive</b>	UK	Remarketing	Data transferred	First name and last name, email address	Combine browsing information with information provided by SecuTix to convince internet user who has abandoned his	No

Type	Name	Country	Activity	Type of data transfer	Data description	Processing description	Agreement with subcontractor
						basket to resume it.	

## Appendix 2.2 Sub-processors that don't have access to end customer personal data

Type	Name	Country	Activity
<b>Other contractors for commercial and technical support</b>	<b>Softjourn, Inc</b>	Ukraine	Software development and integration
<b>Technical partners – Payment</b>	<b>Datatrans</b>	Switzerland	Payment service provider
	<b>Saferpay</b>	Switzerland	
	<b>Masterpass<sup>1</sup></b>	UK	
	<b>Atos</b>	France/Spain	
	<b>RedSys</b>	Spain	
	<b>Logitours</b>	France	
<b>Technical partners – Other</b>	<b>Amazon Web Services</b>	USA	Public file hosting
	<b>Google Maps for Work</b>	USA	Postal address standardisation, validation and auto-suggestion
	<b>Loqate (formerly Pca Predict)</b>	UK	Postal address standardisation, validation and auto-suggestion
	<b>Kulturplanner</b>	Austria	Business intelligence
	<b>3D Digital Venue</b>	UK	3D model of venues (Theater, Stadium...)
	<b>Otipass</b>	France	Manage visit passes valid for multiple venues
	<b>Pacifa 3D</b>	France	3D model of venues (Theater, Stadium...)

<sup>1</sup> Masterpass is only used as a payment method. The internet user has to enter his Masterpass credentials on Masterpass login page. No single sign on between SecuTix and Masterpass.

	<b>PIMS</b>	France	Centralised reporting tool
	<b>Smart Pricer</b>	Germany	Dynamic pricing
	<b>Tech4Team</b>	France	Dynamic pricing
	<b>Two Circles</b>	UK	Business intelligence in sports industry
<b>Ticket reseller</b>	<b>Billetreduc</b>	France	Online sales portal
	<b>Classictic</b>	Germany	
	<b>TickX</b>	UK	
	<b>Tripadvisor Viator</b>	US	