SAP Event Ticketing
## Typographic Conventions

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example</strong></td>
<td>Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Emphasized words or expressions.</td>
</tr>
<tr>
<td><strong>EXAMPLE</strong></td>
<td>Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.</td>
</tr>
<tr>
<td><strong>&lt;Example&gt;</strong></td>
<td>Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.</td>
</tr>
<tr>
<td><strong>EXAMPLE</strong></td>
<td>Keys on the keyboard, for example, <code>F2</code> or <code>ENTER</code>.</td>
</tr>
</tbody>
</table>
Table of Contents

1  Introduction ........................................................................................................................................... 5
2  Before You Start .................................................................................................................................... 6
3  Technical System Landscape ................................................................................................................. 7
4  Security Aspects of Data, Data Flow and Processes ............................................................................ 9
   4.1 Online Shop Sales Process ................................................................................................................. 9
   4.2 Box-Office Sales Process ...................................................................................................................... 9
   4.3 Security Aspects ................................................................................................................................... 10
5  User Administration and Authentication ............................................................................................. 11
   5.1 User Management ............................................................................................................................... 11
   5.2 Authentication .................................................................................................................................... 11
   5.3 Password Security ............................................................................................................................... 12
6  Authorizations ........................................................................................................................................... 13
7  Session Security Protection .................................................................................................................... 16
8  Network and Communication Security ................................................................................................. 17
   8.1 Communication Channel Security ..................................................................................................... 17
   8.2 Network Security .................................................................................................................................. 18
9  Virus Protection ....................................................................................................................................... 19
10 Data Storage Security ............................................................................................................................ 20
11 Data Protection ....................................................................................................................................... 21
   11.1 Data Security Officer .......................................................................................................................... 22
   11.2 Capture Explicit User Consent Before Collecting Any Personal Data ................................................. 24
   11.3 Log Changes to Personal Data .......................................................................................................... 25
   11.4 Log Read Access to Sensitive Personal Data ..................................................................................... 26
   11.5 Provide a Retrieval Function ............................................................................................................ 28
   11.6 Erase Personal Data ........................................................................................................................ 28
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Security-Relevant Information</td>
<td>31</td>
</tr>
<tr>
<td>Security-Relevant Logging and Tracing</td>
<td>32</td>
</tr>
<tr>
<td>Appendix</td>
<td>33</td>
</tr>
</tbody>
</table>
1 Introduction

⚠️ Caution

This guide does not replace the administration or Administration Guide that are available for productive operations.

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guide, Configuration Guide, Administration Guide or Migration Guide. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guide provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the internet for managing business data, the demand on security is also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. The demand on security applies likewise to SAP Event Ticketing. To assist you in securing SAP Event Ticketing, we provide this Security Guide.

About this Document

The Security Guide provides an overview of the relevant security information that applies to SAP Event Ticketing.
2 Before You Start

Configuration
You can find a summary of the configuration steps for implementing security for SAP Event Ticketing in the Configuration Guide. See https://help.sap.com/viewer/p/SAP_EVENT_TICKETING > Configuration.

Additional Information
For more information about specific topics, see the Quick Links as shown in the table below.

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on SAP Service Marketplace or SCN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td><a href="http://scn.sap.com/community/security">http://scn.sap.com/community/security</a></td>
</tr>
<tr>
<td>Security Guides</td>
<td><a href="http://service.sap.com/securityguide">http://service.sap.com/securityguide</a></td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td><a href="http://support.sap.com/notes">http://support.sap.com/notes</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://support.sap.com/securitynotes">http://support.sap.com/securitynotes</a></td>
</tr>
<tr>
<td>Released platforms</td>
<td><a href="http://support.sap.com/pam">http://support.sap.com/pam</a></td>
</tr>
</tbody>
</table>
3  Technical System Landscape

Use

The SAP Event Ticketing system was designed as a web-based thin-client solution. It is based on a three-tier architecture. The system runs on a LAMP (Linux, Apache, MariaDB, PHP) structure. Persistence is realized with a relational database.

On data tier level, the system uses an object-relational-mapping. Therewith any function can also use objects for data related processes. An object cache saves a variety of objects temporarily in shared memory segments of the servers. This object cache builds a database and accelerates system performance.

The GUI-Layer also known as presentation tier has a simple workflow management for all sales related processes. In this layer functionality and presentation is strictly separated. With HTML templates, the sales process can be designed with regards to layout and functionality. Additionally, the GUI layer supports the communication from the SAP Event Ticketing system to other systems based on web services. This also means that all web services only access the business logic and not any data directly.

A CRUD framework allows fast and efficient design of administration dialogs for all components of the system.

Only little functionality resides on client side. This slim functionality is mainly represented as JavaScript code or as the so-called SAP Event Ticketing Local system.
Since SAP Event Ticketing deals with business data from your core business processes, SAP adheres to the highest security and quality requirements, as follows:

- The business data is stored securely in SAP data centers.
- Users who require access to the business data must authenticate themselves, and their identity must be verified by user and access management.
- Customer data always belongs to the customer.

Industry best practices and state-of-the-art open cryptographic standards secure and protect communications between customer devices and the system landscapes of your SAP Event Ticketing solution in the SAP data center.

To access SAP Event Ticketing, you must enter a unique, customer-specific URL.
4 Security Aspects of Data, Data Flow and Processes

The following 2 chapters explain and visualize the 2 main sales processes in SAP Event Ticketing. The usages of external systems (show as blue rectangles) and other SAP products are examples. In the end, the SAP Event Ticketing system can work ‘stand-alone’, without any connection to other systems.

4.1 Online Shop Sales Process

In this case, the sales process is initiated by a web user who accesses the SAP Event Ticketing online shop.

4.2 Box-Office Sales Process

This process is a typical ticket sale at a box office, which is initiated by a sales agent at the box-office.
4.3 Security Aspects

There are various security aspects considered in SAP Event Ticketing regarding processing or storage of data. This section provides an overview; details are provided in the appropriate chapters of this document.

Process-related security aspects include:

- All connections to the application server are secured using the https protocol.
- The database is password protected to secure it from unauthorized access.
- All users must provide their credentials on the login screen.
- All SAP Event Ticketing APIs are secured with a security token. This security token will be generated during the registration of a shop and will be returned to the caller.
- Data considered personal data:
  - Customer data (name, address, etc.)
- Data considered sensitive data:
  - Bank data (optional)
5 User Administration and Authentication

5.1 User Management

Use

Users and user rights are defined with the user management function that is integrated into SAP Event Ticketing.

User Types

Different user types exist in SAP Event Ticketing for different purposes:

- **Ticket**: The user type for normal business / dialog users.
- **Transfer**: A special user type which is used for server to server ticket transfer communication.
- **Technical User**: The user type which is used for interface / API communication arrangements.
- **Guard User**: A special user type which is used for guard access control communication.
- **Data Security Officer**: A special user who respects the provisions of applicable data protection laws.

5.2 Authentication

Every user type must authenticate itself to SAP Event Ticketing for regular browser-based front-end access, as well as for electronic data exchange, such as business-to-business communication. SAP Event Ticketing does not support anonymous access.

When a new user is created, a user ID is created.

Users log on to SAP Event Ticketing with their assigned user ID and password.
5.3 Password Security

You as an administrator can set an initial password and edit and create security policies according to the security requirements of your company. You set up password checks on the tab page Master Data > Company under Back-end Password Complexity. The default setting of all the fields is zero. This means that the password properties are not checked.

It is recommended to check and harden the security policy for passwords which is pre-configured in your solution. For more information, see the SAP Event Ticketing Configuration Guide (https://help.sap.com/viewer/p/SAP_EVENT_TICKETING > Configuration.).
## 6 Authorizations

### Use

Authorizations in SAP Event Ticketing are configured via single user rights or so-called right groups.

### Role and Authorization Concept for <Application>

The authorization concept in SAP Event Ticketing is realized by

- **Single user right:**
  This is a single authorization which is represented by a single, distinct setting.

- **Rights group:**
  This is comparable to a user profile in other SAP products which are based on SAP NetWeaver.
  A rights group is a full configuration set of all available user rights

You can assign both user rights (authorizations) and rights groups on user level.

Rights management contains a range of cumulative authorizations. No rights are assigned to new users with the standard role. These new users can only use the functions for ticket sales. Any additional rights granted must be in line with the user's tasks. Note that some tasks require several rights.

You create the rights groups in the company master data on the Master Data tab page, under Company Select Company > Rights Group.

There are no pre-defined rights groups in SAP Event Ticketing.

The table below lists the various user rights and how they relate to one another:

<table>
<thead>
<tr>
<th>Number</th>
<th>Right</th>
<th>Requires Right with Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Master Data</td>
<td>None</td>
<td>Activates the Master Data tab page.</td>
</tr>
<tr>
<td>2</td>
<td>Event Series</td>
<td>1</td>
<td>The users can create and manage events.</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number</td>
<td>Right</td>
<td>Requires Right with Number</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Venue Administrator</td>
<td>1</td>
<td>The users can create and manage venues.</td>
</tr>
<tr>
<td>4</td>
<td>Event Administrator</td>
<td>1</td>
<td>If price lists, venues, and event series exist, the user can manage events and create them to a certain extent. Otherwise, rights 2, 3, 7, and 8 are also required to create events.</td>
</tr>
<tr>
<td>5</td>
<td>Company Administrator</td>
<td>1</td>
<td>The user can manage his or her company and create subordinate companies. The user can also create online shops. Note An online shop can become operational only if an appropriate Internet user exists (right 6).</td>
</tr>
<tr>
<td>6</td>
<td>User Administrator</td>
<td>1, 5</td>
<td>The users can create and manage company users.</td>
</tr>
<tr>
<td>7</td>
<td>Price List Administrator</td>
<td>1</td>
<td>The users can create and manage company price lists.</td>
</tr>
<tr>
<td>8</td>
<td>Region/City Administrator</td>
<td>1</td>
<td>The users can create and manage cities.</td>
</tr>
<tr>
<td>9</td>
<td>Superadmin/Operator</td>
<td>None</td>
<td>Activates the System tab page.</td>
</tr>
<tr>
<td>10</td>
<td>Language Administrator Rights</td>
<td>None</td>
<td>The user can edit language entries on the user interface that are</td>
</tr>
<tr>
<td>Number</td>
<td>Right</td>
<td>Requires Right with Number</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11</td>
<td>System Administrator</td>
<td>1, 5</td>
<td>All events and event series in the pool restrictions are visible only to system administrators.</td>
</tr>
<tr>
<td>12</td>
<td>Customer Card Manager</td>
<td>None</td>
<td>Activates the Members/Tickets tab page. Users with this right can manage memberships and clubs.</td>
</tr>
<tr>
<td>13</td>
<td>SAP Event Ticketing Admin</td>
<td>None</td>
<td>Activates the SAP tab page.</td>
</tr>
</tbody>
</table>
7  Session Security Protection

Once a user has logged on to the system (backend) or once a user has accessed the online shop, the system assigns a session ID to the user and saves it in the database. The system automatically deletes the session after a defined period of inactivity. The session ID is generated and maintained by the system in a secure and not guessable manner provided by the framework.

Additionally a cookie-based security token can be enabled within the backend for all shops which will be a second security mechanism if needed. This will for example prevent that end-customers accidentally send their active session to others and the session gets compromised.
8 Network and Communication Security

SAP Cloud Trust Center

8.1 Communication Channel Security

Use

The table below shows the communication channels used by SAP Event Ticketing, the protocol used for the connection, and the type of data transferred.

<table>
<thead>
<tr>
<th>Communication Path</th>
<th>Protocol Used</th>
<th>Type of Data Transferred</th>
<th>Data Requiring Special Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front-end client with browser to application server</td>
<td>HTTPS</td>
<td>All application data</td>
<td>Passwords and bank details</td>
</tr>
<tr>
<td>Front-end client uses interfaces to application server</td>
<td>XMLRPC/SOAP</td>
<td>All application data</td>
<td>Passwords and bank details</td>
</tr>
<tr>
<td>Application server to MariaBD database</td>
<td>TCP/IP</td>
<td>All application data</td>
<td>Passwords and bank details</td>
</tr>
<tr>
<td>SAP Event Ticketing Local</td>
<td>HTTPS</td>
<td>All application data</td>
<td>None</td>
</tr>
</tbody>
</table>

HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. XMLRPC/SOAP connections are protected with Web services security using the following mechanisms to ensure that only authenticated users have access to the system:

- A user / an application logs on to the system; if this is successfully authenticated, the system assigns a session ID. I.e. the application that uses the interface generates a session in the same way as a regular backend user when logging on to the system: This involves specifying the company identifier, user identifier, and password.
This means that authorizations are managed in the same way as for all points of sale and shops. This simplifies the overview and facilitates use without compromising on security in this area.

- The system requires a session ID for every request to the system. If the session ID is valid, the system grants access to the request. If the session ID is invalid, the system rejects the request.

8.2 Network Security

Use

The network infrastructure for your SAP Event Ticketing solution contains several security technologies. The multilayered, partitioned, proprietary network architecture permits only authorized access to the data centers that support your SAP Event Ticketing solution, with features that include:

- A Web dispatcher farm that hides the network topology from the outside world
- Multiple internet connections to minimize the impact of distributed denial-of-service (DDoS) attacks
- An advanced intrusion detection system that continuously monitors solution traffic for possible attacks
- Multiple firewalls that divide the network into protected segments and shield the internal network from unauthorized internet traffic
- Third-party audits performed throughout the year to support early detection of any newly introduced security issues
9  Virus Protection

You can upload attachment files to your SAP Event Ticketing solution in several application scenarios. Regularly updated antivirus software checks the uploaded files for viruses and other types of malicious software. SAP checks each file during the upload. A corresponding error message will be shown if a virus is detected. The file will only get stored to the system if no virus was found.
10 Data Storage Security

Use

The system stores data in MariaDB databases and in the file system of the application server. Except for user passwords, this data is not encrypted in the database. Data is saved for every transaction. Users can upload files (such as images) to the system using the corresponding functions. Depending on their size, the system saves these files in the database as a binary large object or, if a certain size limit is exceeded, in the file system of the application server. When a file is stored in the file system, the actual file name is replaced by a unique name. This ensures that it is not possible to determine the content of an image file based on the file name, for example.
11 Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

Note

In the majority of cases, compliance with data privacy laws is not a product feature.

SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data.

SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Information about an identified or identifiable natural person.</td>
</tr>
<tr>
<td>Business purpose</td>
<td>A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.</td>
</tr>
<tr>
<td>Blocking</td>
<td>A method of restricting access to data for which the primary business purpose has ended.</td>
</tr>
<tr>
<td>Deletion</td>
<td>Deletion of personal data so that the data is no longer usable.</td>
</tr>
</tbody>
</table>
Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

**Access control**: Authentication features as described in section 5. User Administration and Authentication.

**Authorizations**: Authorization concept as described in section 5. User Administration and Authentication.

**Read access logging**: as described in section 11.2 Read Access Logging.


**Input control / Change logging**: Change logging is described in the application-specific documentation.

**Configuration of Data Protection Functions**

Certain central functions that support data protection compliance are available within the application. Activate the new Software Configuration value `global_data_privacy` under menu entry `System > System Configuration > Software Configuration`.

For more information on setting up data protection, please see the following pages.

### 11.1 Data Security Officer

**Introduction**

Certain data protection and privacy laws require special security measures to be implemented when collecting, processing, and/or using personal data. SAP delivers functionalities to our customer to help them to comply with native requirements.
The customers data security officer acts on compliance with the provisions of the applicable data protection laws. The data security officer will continue to be responsible for the implementation of the Directives and the associated standards and guidelines in the relevant area.

- A central role of the data security officer can be set up in SAP Event Ticketing.
- The function of this role is to define an organizer/company as a data security officer and thus assign responsibility for data protection within the company to designated employees.
- SAP Event Ticketing offers the organizer the possibility to appoint a data security officer at client / company level.
- SAP Event Ticketing assists organizers in complying with the applicable data protection regulations, but this does not include legal advice.

Use

You assign the right of the data protection officer to a user. The right can be assigned directly in the user or via a rights group.

The rights assigned to it can be used in connection with the chameleon rights.

The data security officer can use the chameleon rights to perform settings in a company, even if the company does not have its own data security officer!

The data security officer's right includes the right for the following actions and administrations.

The data security officer can assign data protection related rights to users.

- reading/ exporting change histories
- Create overview of data from individuals
- Indication of a customer for deletion/anonymization
- The data security officer has the right to administer the company's privacy settings.
- The data security officer can block and reactivate customers.
- The data security officer can delete/anonymize customer data.

Notes

If there is no user in a company with the right for the data security officer, the following warning is displayed in the company dialog.
11.2 Capture Explicit User Consent Before Collecting Any Personal Data

Introduction

A person affected must be informed in a suitable manner that their personal data is being collected, processed, and/or used. Usually, they are to be informed before the time at which data is collected.

The person affected must be informed of the company collecting the data, the purpose for collecting, processing, or using the data, as well as other recipients to whom their data will be transferred. The information must be provided in a way that is easy to understand.

Stored personal data must be accurate. Inaccurate data must be corrected or deleted as soon as practicably possible.

All processes for collecting, processing, and/or using personal data must contain an option for correcting, updating, and, where required by applicable law, deleting or blocking.

Data Storage Checkbox

The customer is requested in the system to agree to the general terms and conditions. This takes place in the webshop during the sales/purchase process.

Furthermore, the system asks the new customer/consumer for consent to the collection of personal data when registering for ticket transfer (accept ticket transfer).

If the customer does not accept the agreement (general terms and conditions), the system prevents the acceptance of the ticket transfer and does not save the customer data.

If you activate this setting, the confirmation of the data protection guidelines is requested in the WOW-Shop template set under the function Login/Register.

You will need to confirm this to proceed with registration.

This confirmation must also be made in the shopping cart, in case a shopping cart is created without login and the customer wants to register via the shopping cart.

Marketing Declaration of Consent and Communication Block

Before you can send an e-mail to a customer, you first need to ensure that the legal basis is in place. SAP Event Ticketing supports you in complying with all legal requirements arising from the data protection regulations of the European Union:

- Obtaining marketing declarations of consent from the customer
- Option to register for standard forms of communication and newsletters in the online shop
• Option to set up general communication blocks for any customers who want to be excluded from such communication

You can find the customer registrations in the communication matrix in the customer master data of the customer in question. Here, you can cancel registrations or add new registrations.

Note

The registration is not sufficient for sending newsletters or other standard forms of communication. This always requires the marketing declaration of consent.

You can set a general communication block for a customer if the customer has selected the option indicating that it does not want to receive any advertisements or information, regardless of the communication channel used. The system evaluates the general communication block when a mailing job is created in step 2.

For setting statistics, a business object named Marketing Declaration of Consent is available below the Customer business object.

The individual attributes are assigned to the business object Marketing Declaration of Consent.

• Validity
• Marketing type
• Communication channel
• Agreement date
• Objection date

11.3 Log Changes to Personal Data

Integration

SAP Event Ticketing records a customer’s personal data. The history provides information on which personal data has been collected and changed. SAP Event Ticketing records information for each data record in the system, the date and time of the change, the changed values in the data record, the processor and also Source and Purpose is logged.

The history enables the organizer to see and check changes. Access to the history is controlled by the data security officer. Passwords are not logged visibly. The history is user-friendly at the menu items.
Use

During the booking process the SAP Event Ticketing system records customers’ personal data. Data recording is logged, i.e. the system records a history of customer data creation and changes, as well as of which user has modified the data.

It also records the date when data was entered or changed. When changes are made, the system also records the data itself. This data can be called up in the customer dialog via the "History" icon in the title row.

Settings history

The relevant settings for data protection are also logged. The history icon in the respective dialog gives you access to it.

- Dialogue User
- Data Privacy Settings Dialog Box
- Chameleon users

Calling up the history opens a dialog. You can restrict the data search by using search criteria.

In the customer dialog itself you can access the entire customer history, i.e. the history of additional addresses, bank details, memberships, etc. You can restrict the search by the object type.

You can call the history of individual objects (e.g. a specific additional address or payment method) by using the history in the relevant sub dialog. In this case you do not have to select the object types.

If the system setting for data protection is not activated at system level, the change log for customer data is output to each system user who can see/create the customer.

The system logs the user and the company that change the data.

Only system users who have the right to access the log records (customer data logs) can view/download the change log.

11.4 Log Read Access to Sensitive Personal Data

Introduction

Sensitive personal data are for example information about racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life. Sensitive personal data shall be treated in the same way as such personal data which constitute a special level of protection for the persons concerned. If SAP Event Ticketing personal data is collected, it must be ensured that the persons concerned have been informed in advance and have given their consent.
Caution

The collection, processing or use of personal and sensitive personal data at recognizably inadmissible places, such as free text fields, are not intended for this use. In the interest of data protection, this should be avoided.

Use

Log read access to sensitive personal data

In order to comply with the data protection regulation and to enable access to logged data, the activation and administration of user rights for the data security officer is necessary. According to this right, the following actions can be performed:

In SAP Event Ticketing, we log for example the date, time, company, user, old information, new information on specific customer data, bankdata and nationality.

Reading/exporting change histories

- Create overview of data from individuals
- Indication of a customer for deletion/anonymization

These rights will be deactivated as long as the right to act as data security officer is not assigned!

History of customer data

Access to the entire customer history is possible in the customer dialog, which also means that the history of additional addresses, bank data, memberships, nationality etc. can be viewed here. You can restrict the search using the object type.

Customer data object types

You can call the history for the individual objects - a specific additional address or a payment method - in the history in the corresponding subordinate dialog. Here you do not need to select the object type.

In the customer dialog itself, access to the entire customer history is possible, i.e. the history of additional addresses, bank data, memberships etc. can also be viewed here. You can restrict the search using the object type.
11.5 Provide a Retrieval Function

Introduction
With the matching user rights, all personal data of a customer can be displayed and export to a report, to send it to the customer.

Use
In the Customer area, you can call up and edit the customer data records entered in the system for individual and corporate customers or create new customer data records. In addition to basic data such as name and address, you can also enter customer memberships, set up payment methods or assign customers to a customer group in order to facilitate ticket sales.

The system enables you to enter or edit additional customer data for a customer data record. For example, you can enter payment methods such as bank details or credit cards, create additional addresses or upload images. These supplementary customer data support and facilitate ticket sales and customer advice.

Applications that store personal data provide a function, to report or display, the personal data about the data subject. By default, the function contains any data that is foreseen as personal data about the data subject to be stored by the SAP software. The report shall be configurable and extensible by the customer. Access to the function shall be restricted by adequate authorizations.

SAP Event Ticketing provides a function that reports and displays personal data. The report function is configurable and extensible for all data and for all selected data. This makes it possible to create a report on all selected data that is stored in the system via a customer/person.

The data security officer may give users the right to access the reports and data. He can manage this right and deactivate it for certain users.

A user authorized by the data security officer can export the report / results list as xml, pdf based on the selected selection of customer data. This access to customer data by the authorized user is logged accordingly.

The report contains the displayed / downloaded data as follows.

- The source of the data (database, webshop, interface external system)
- The recipients or categories of recipients to whom the data is transmitted (interfaces only)
- The purpose of data storage (e.g. ticket purchase, membership, ticket transfer, resale, interface).

11.6 Erase Personal Data

Integration
The erase of personal data can take place in the SAP Event Ticketing after expiry of the specified retention period. This is the task of the data security officer. This identifies the customers for erase. Personal data can be made anonymous after expiry of the specified retention period and can no longer be used.

The contents of the erased data can no longer be viewed in the history. The erase of personal data is done in the SAP Event Ticketing by a function. The marked data are anonymized or erased with the help of mass data processing.

A person concerned may at any time request information about the data stored on his or her person, their origin, purpose of storage and the recipient to whom the data is passed on. It is also possible to request the erase or deactivation of personal data.

Use

In the system, the data security officer can set a time period in which inactive customers (no transaction during this time period and the customer has no marketing authorization or newsletter subscription) are erased/deactivated at the company level.

Furthermore, he can enable/disable a user privilege to mark a customer/user as erase/anonymous. An authorized user is supported so that a customer can be erased (anonymously) in the back office.

The system checks whether the customer can be marked as “to be erased/anonymized” and if this is not possible, an error message is issued.

It is not possible to erase/anonymous a customer if a transaction is still active or has subscribed to an active newsletter or marketing authorization and active membership.

A customer that has been erased or anonymized in the system is not found in the back office and cannot be used there. A customer who has been erased/anonymized in the system cannot log on to the webshop and use his data there.

Erased/-anonymous customers are also displayed anonymously in statistics and reports. In the system, the data security officer can set a period of time for how long invoices are stored in the system. This is done at company level.

Customer data is automatically flagged for erase in the proposal list. This is done when the period of inactivity of the customer is reached, no transaction has occurred in a certain period of time, no active marketing authorization/newsletter registration is available and the period of storage of invoices is reached.

You can export the proposal list for erase (xml, pdf, browser display), the conditions are taken into account. The data security officer has the possibility to erase customer data marked as "erase/anonymize".

A change of the customer status from active to erased is logged in the history with anonymous data. In the history, only the erase is displayed and all other stored data are erased.
Note

Blocked / erased customer data are not transferred to connected systems (ERP, CRM, Access......).

The following functions are available for setup

Time Period for Erasure of Inactive Customers in Days - Definition of retention periods for the administration of personal data

Time Period for Erasure of Invoices in Month - Definition of retention periods for the administration of personal data
12 Other Security-Relevant Information

Security Check of Data Entries

SAP Event Ticketing is a web-based server software that provides administration and sales screens via a web browser. To safeguard the security of the software and the stored data, entries made in the entry and form fields of SAP Event Ticketing are subjected to a security check. This check prevents the entry of certain characters and character strings.

In the main check function, the following characters are removed or replaced with blanks:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>opening parenthesis</td>
</tr>
<tr>
<td>)</td>
<td>closing parenthesis</td>
</tr>
<tr>
<td>&lt;</td>
<td>opening angle bracket, less than</td>
</tr>
<tr>
<td>&gt;</td>
<td>closing angle bracket, greater than</td>
</tr>
<tr>
<td>`</td>
<td>grave accent, back quote, back quote</td>
</tr>
<tr>
<td>&amp;</td>
<td>ampersand</td>
</tr>
<tr>
<td>=</td>
<td>equals</td>
</tr>
<tr>
<td>[</td>
<td>opening bracket</td>
</tr>
<tr>
<td>]</td>
<td>closing bracket</td>
</tr>
<tr>
<td>&lt;xyz&gt;</td>
<td>String is deleted</td>
</tr>
</tbody>
</table>

Also, adjusted versions of this main check function exist to enable the functionality and requirements of certain predefined entry fields in the back office.

Passwords are stored separately and are subject to a separate security check.
13 Security-Relevant Logging and Tracing

Change History

Mainly in the ticket booking process but also in other processes (e.g. membership processes), customer data is stored and maintained in SAP Event Ticketing.

Changes of customer data are logged, i.e. the system records a history of customer data creation and changes, as well as which user has modified the data. It also records the date / timestamp of the activity. When changes are made, the system also records the data itself. This data can be called up in the customer dialog via the "History" icon in the title row.

In the history dialog, you can restrict the data search by using search criteria.

History data can be retrieved and displayed on different levels - either for the entire customer or for single sub-objects (like a specific address or a single membership).
14 Appendix