

# SAP Sports One



# Typographic Conventions

Type Style	Description
<b>Example</b>	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.
<b>Example</b>	Emphasized words or expressions.
<b>EXAMPLE</b>	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.
<b>Example</b>	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.
<b>Example</b>	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<b>&lt;Example&gt;</b>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
<b>EXAMPLE</b>	Keys on the keyboard, for example, <b>F2</b> or <b>ENTER</b> .

---

## Document History

Version	Date	Change
0.9	2017-06-20	Initial version
1.0	2017-07-17	1 <sup>st</sup> published version
1.1	2017-09-20	Update: Deletion of Personal Data
1.2	2018-01-05	Revoke User Consent and Terms of Use
1.3	2018-04-12	User Consent for Mobile Apps
1.4	2018-11-27	Language Revision

---

# Table of Contents

1	Introduction .....	6
2	Before You Start .....	8
3	Technical System Landscape .....	9
3.1	Overview .....	9
3.2	Hardware and Software Requirements .....	10
4	User Administration, Authentication, and Authorizations .....	12
4.1	User Management.....	12
4.2	Authorizations .....	13
5	Session Security Protection.....	16
6	Network and Communication Security .....	17
7	Application-Specific Virus Scan .....	18
8	Data Storage Security.....	19
9	Data Protection .....	20
9.1	Deletion of Personal Data .....	21
9.2	Read Access Logging and Change Access Logging .....	22
9.3	Personal Data Report .....	23
10	Consent Management.....	24



---

# 1 Introduction



## Caution

SAP Sports One is a cloud product, therefore the architectural details and security measurements are subject to change.

In case you need any clarification, please open a support ticket in the following component: IS-SE-SPS.

## Target Audience

- Data security officer
- Technology consultants
- Security consultants
- System administrators

This document provides 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 demands on security are 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. These demands on security apply likewise to SAP Sports One. To assist you in securing SAP Sports One, we provide this Security Guide.

## About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Sports One. SAP Sports One consists of a [Web Application](#) and several dependent [Mobile Applications](#). This guide contains an overview and detailed, security-relevant information for all dependent applications.

---

## Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**

This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.
- **Technical System Landscape**

This section provides an overview of the technical prerequisites, components, and communication paths that are used by SAP Sports One and the technical prerequisites.
- **User Administration, Authentication, and Authorizations**

This section provides an overview of the following user administration and authentication aspects:

  - Recommended tools to use for user management
  - Overview of the authorization concept that applies to SAP Sports One
- **Session Security Protection**

This section provides information about activating secure session management, which prevents JavaScript or plug-ins from accessing the SAP login ticket or security session cookies.
- **Network and Communication Security**

This section provides an overview of the communication paths used by SAP Sports One and the security mechanisms that apply.
- **Application-Specific Virus Scan**

This section provides an overview of activated, application-specific virus scan profiles and their behavior.
- **Data Storage Security**

This section provides an overview of any critical data that is used by SAP Sports One and the security mechanisms that apply.
- **Data Protection**

This section provides information about how SAP Sports One protects personal or sensitive data.
- **Consent Management**

This section provides an overview of how to handle Terms of Use documents and request user consent from different user groups.

## 2 Before You Start

### Fundamental Security Guides

SAP Sports One is built on top of an [SAP HANA Database](#) and hosted in the [SAP Cloud Platform](#). The underlying database version is updated regularly by SAP Operations. Optionally, it is possible to connect [SAP Analytics Cloud](#) directly to the [SAP HANA Database](#) for business intelligence, planning, and predictive analytics purposes. Therefore, the following security guides might be of interest:

#### Fundamental Security Guides

Scenario, Application, or Component Security Guide	Most Relevant Sections or Specific Restrictions
<a href="https://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf">SAP HANA Security Guide</a> <a href="https://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf">https://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf</a>	User Management
<a href="https://help.sap.com/viewer/p/SAP_BusinessObjects_Cloud">SAP Analytics Cloud</a> <a href="https://help.sap.com/viewer/p/SAP_BusinessObjects_Cloud">https://help.sap.com/viewer/p/SAP_BusinessObjects_Cloud</a>	Help Document → Security
<a href="https://cloudplatform.sap.com/capabilities/security.html">SAP Cloud Platform</a> <a href="https://cloudplatform.sap.com/capabilities/security.html">https://cloudplatform.sap.com/capabilities/security.html</a>	

### Important SAP Notes

SAP Sports One is hosted in the SAP Cloud Platform. The software is updated regularly with new business functionality, software corrections, and security patches. Therefore, security-relevant SAP Hot News and SAP Notes are not published.

### Configuration

You can find configuration steps for implementing security for SAP Sports One in this document and in the standard documentation for [SAP Sports One](#).

### Additional Information

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

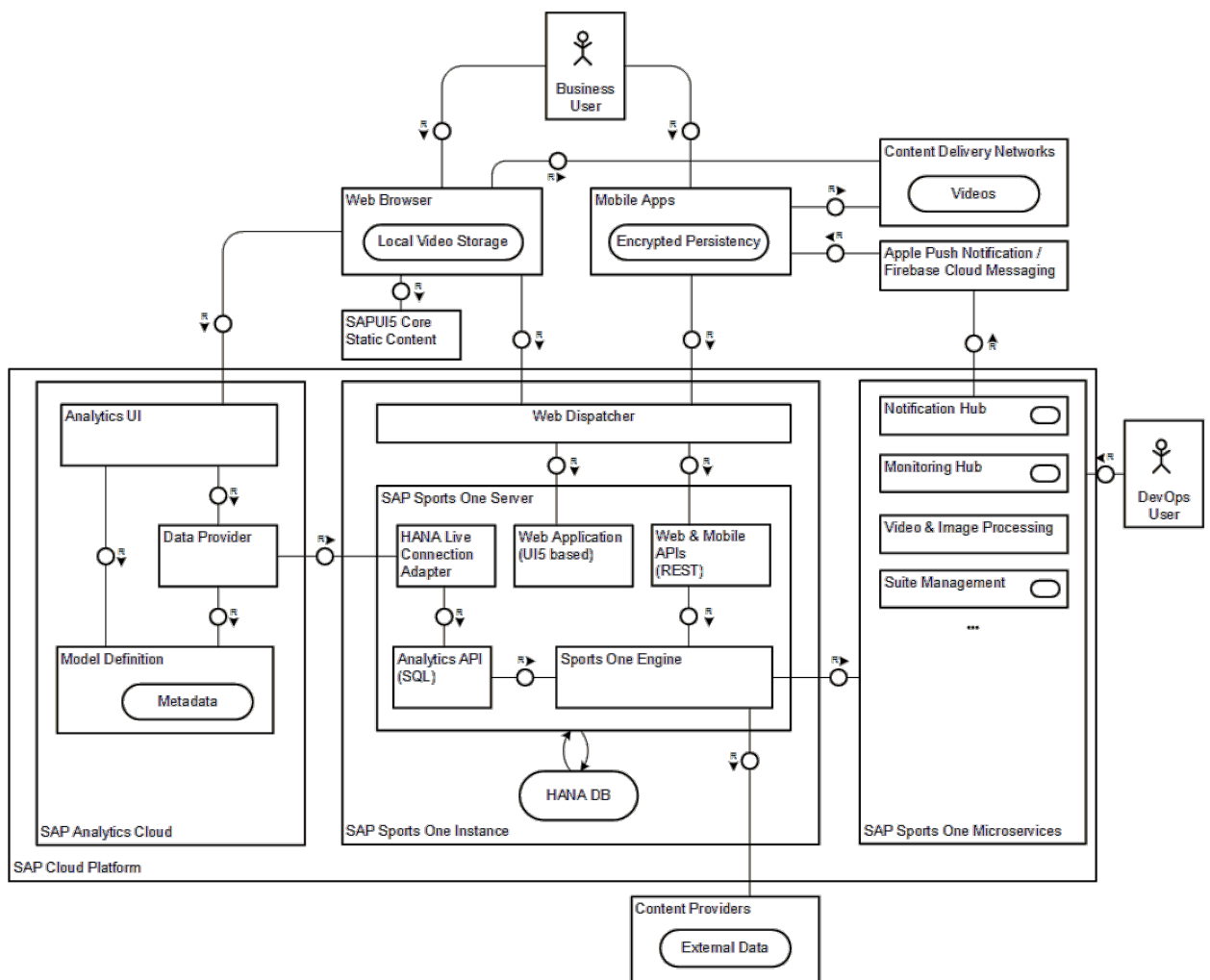
Content	Quick Link on SAP Service Marketplace or SCN
Security	<a href="http://scn.sap.com/community/security">http://scn.sap.com/community/security</a>
Security Guides	<a href="http://help.sap.com">http://help.sap.com</a> search for security guide



## 3 Technical System Landscape

### 3.1 Overview

The figure below shows an overview of the technical system landscape for SAP Sports One:



The **SAP Sports One** product consists of frontend applications that communicate with the cloud backend using restful services. Videos are streamed to the frontend applications directly from a **Content Delivery Network (CDN)**.

The frontend applications consist of a **Web Application** (SAP Sports One - Web App) based on the SAPUI5 user interface control library as well as native **Mobile Applications** (SAP Team One, SAP Challenger Insights, and SAP Player Fitness).

Static SAPUI5 user interface control library artefacts are served from a central cloud service. The Web App itself and all restful data services are provided by an SAP Sports One Server sitting on top of an **SAP HANA Database**.

The system stores large amounts of master data and transactional data for analytic processing. Whilst some of the data can be entered manually, the bulk is imported from external content providers.

The system makes use of [SAP Sports Micro-Services](#) like a [Notification Hub](#) in the cloud to broker notifications to mobile devices using Apple Push Notification Service or Firebase Cloud Messaging.

Optionally, it is possible to connect [SAP Analytics Cloud](#) directly to the [SAP HANA Database](#) for business intelligence, planning, and predictive analytics.



**Caution**

SAP Sports One is a full web-based offering. You will need an Internet connection and a system that meets certain requirements. Before you start to use SAP Sports One check the requirements and recommendations in this section. The requirements listed in this chapter are for the current release.

## 3.2 Hardware and Software Requirements

### Client Software Requirements

Client Software	Version	Additional Information
Desktop browser	Google Chrome	Google releases continuous updates to their Chrome browser. We make every effort to fully test and support the latest versions as they are released. However, if defects are introduced with OEM-specific browser software, we cannot guarantee fixes in all cases. If you have a question about a specific version (for example whether a specific version is supported), please log a support ticket.  For additional system requirements, see your web browser documentation.
Operating system		SAP Sports One is not dependent on any specific operating system. All capabilities are accessible through a web browser.  For additional system requirements, see your operating system documentation.
Additional software	PDF Reader	SAP Sports One generates PDF documents in several business functions, therefore a PDF reader like Adobe Acrobat Reader is required.  For additional system requirements, see your PDF reader system documentation.
Additional software	Spreadsheet Software	SAP Sports One generates and imports spreadsheet documents in several business functions, therefore Spreadsheet Software like Microsoft Excel is required.  For additional system requirements, see your spreadsheet software documentation.

### Client Configuration Requirements

Client Configuration	Setting	Additional Information
Network bandwidth	Recommended connection speed 16Mbits or faster	In general, SAP Sports One requires no more bandwidth than is required to browse the Internet. All application modules are designed for speed and responsiveness with minimal use of resources.
Screen resolution	Minimum 1280px screen width	Aspect ratio 16:10 - 1280x800 or higher Aspect ratio 16:9 - 1366x766 or higher (widescreen) Aspect ratio 4:3 – 1280x960 or higher
JavaScript	Enabled	
Pop-up windows	Allow pop-up windows	Allow pop-up windows from the SAP Sports One domain

#### Supported Languages

Client Browser	Setting	Additional Information
Menus, buttons, messages, and other elements of the user interface	cs, cs_CZ de, de_DE en, en_US, en_GB es, es_MX fr, fr_FR hr, hr_HR hu, hu_HU it, it_IT pl, pl_PL sk, sk_SK zh, zh_CN	Supported languages: Czech (cs), German (de), English (en), Spanish (es), French (fr), Croatian (hr), Hungarian (hu), Italian (it), Polish (pl), Slovak (sk), Simplified Chinese (zh)  The language is derived from the desktop browser language and locale setting.  For additional information, see your web browser documentation.

#### Mobile Requirements

Hardware and Software	Additional Information
iOS device	Requires iOS 10.0 or later. Compatible with iPhone and iPad only.  Requires iOS mobile device with 2 GB of RAM or more (iPhone 6s or later, iPad Air 2 or later, iPad Pro). For the best experience, use a mobile device with a fast processor and a good data or Wi-Fi connection.
Android device	Requires OS version 4.4 (KitKat) or later.  Requires mobile device with 2 GB of RAM or more. For the best experience, use a mobile device with a fast processor and a good data or Wi-Fi connection.

# 4 User Administration, Authentication, and Authorizations

SAP Sports One uses the user management and authentication mechanisms provided with the SAP HANA Database. All security recommendations and guidelines for user administration and authentication as described in the [SAP HANA Security Guide \[SAP Library\]](#) also apply to SAP Sports One.

In addition to these guidelines, we include information about user administration that specifically applies to SAP Sports One in the following topics:

## 4.1 User Management

User management for SAP Sports One uses the mechanisms provided with SAP HANA Database, for example, password policies, user validity periods, or allowed user names. For an overview of how these mechanisms apply to SAP Sports One, see the sections below.

### User Administration Tools

The table below shows the tools to use for user management and user administration with SAP Sports One. All tools listed below are available in the SAP Sports One Web Application.

#### User Management Tools

Tool	Detailed Description	Prerequisites
<a href="#">User Management</a> <a href="#">Admin</a> → <a href="#">Users</a>   <a href="#">Users</a>	Create and delete individual users, assign roles and permissions, define validity periods, and generate an initial or reset a password.	<a href="#">Administrator Role</a> within <a href="#">SAP Sports One</a>
<a href="#">User Management</a> <a href="#">Admin</a> → <a href="#">Users</a>   <a href="#">Functions</a>	Create a team user for Match Insights presentation mode. This user is automatically assigned the team kiosk role for Match Insights presentation mode.	<a href="#">Administrator Role</a> within <a href="#">SAP Sports One</a>
<a href="#">Password Policy</a> <a href="#">Data Security</a> → <a href="#">Security Settings</a>   <a href="#">Password Policy</a>	Check the current valid password policies such as the password length and the number of allowed failed login attempts. In case of a change request, open a support ticket.	<a href="#">Data Security Officer Role</a> within <a href="#">SAP Sports One</a>

Tool	Detailed Description	Prerequisites
<a href="#">Change Password</a> <a href="#">Own Settings → Change Password</a>	Every user can change their own password.	<a href="#">SAP Sports One user</a>
<a href="#">User Onboarding</a> <a href="#">Admin → Users   Users</a>	Generate a welcome letter and a password invitation.  Generate a personal onboarding link, optionally secured with a PIN.	<a href="#">Administrator Role within SAP Sports One</a>

One business role – the Administrator – who is the key user of the sports club or federation is authorized to define and maintain the user management and authorization within SAP Sports One. In general, only a very limited number of authorized persons should have the administrative access rights to access user management and authorization tools. The Administrator defines the following for each user:

- A unique user identifier
- Validity period (optional)
- Required business roles
- Instance-based authorization criteria (permissions)

The Administrator also generates an initial password, which each user must change in accordance with the defined password policies. Additionally, Administrators can delete, unlock, and deactivate users on request. The unique user identifier is also used to track user activities for auditing purposes.

Users who are no longer required should be deactivated. The user’s unique user identifier should not be used for new users to maintain the integrity of the data trace.

Before a user can connect to SAP Sports One, the system performs the following checks as part of the login process:

- Authenticates the user using user name or password
- Verifies that the user's account is within its validity period
- Verifies that the user's account is active. It is possible to explicitly deactivate user accounts. Additionally, it might be that a user is inactive due to too many invalid login attempts.

## 4.2 Authorizations

SAP Sports One uses a role-based authorization concept. SAP Sports One users who have been assigned the Administrator role can grant and revoke roles to all SAP Sports One users.

### Note

For more information about how to assign roles, see the [SAP Sports One Documentation](#).

## Role and Authorization Concept for SAP Sports One

### Standard Roles

The table below shows the standard roles that are used by SAP Sports One.

#### Standard Roles

Role	Description
Administrator	Administrator for club or association
Data Security Officer	Data Security Officer for club or association
Manager	Manager of club or association
Coach	Team Coach
Team Manager	Team Manager of team
Player	Team Player
Physiotherapist	Physiotherapist for team
Performance Diagnostician	Performance Diagnostician for team
Match Analyst	Match Analyst for team, club, or association
Scout	Scout for team, club, or association
Chief Scout	Chief Scout for team, club, or association
Team Kiosk Role (for Match Insights)	Presentation mode for SAP Match Insights (*)

(\*) cannot be assigned manually

### Customer-Specific Roles

Currently, it is not possible to define customer-specific roles within SAP Sports One.

### Critical Role Combinations

Technically, there are no critical combinations for the standard roles.

### Permissions

In addition to roles, it is possible to assign permissions to an SAP Sports One user. Permissions restrict access to a subset of data objects and define the data access, for example, if edit or read-only access is allowed.

---

## Mobile Apps

Mobile Apps are connected to the backend system with the same user and password authentication as with the Web Application. Therefore, the user authentication, user authorization, and permissions defined in the SAP Sports One Web Application apply to all SAP Sports One Mobile Apps.

---

## 5 Session Security Protection

The system can, from within the applications, logoff a user. The system automatically terminates the session after a pre-determined time of inactivity.

SAP Sports One mobile applications use the same mechanism and force users to login again and authenticate themselves if the password is not stored in the secure store of the device. If the password is stored in the secure store of the device, the system automatically performs a new login if the session expires.



---

## 6 Network and Communication Security

The SAP Sports One system uses Hyper Text Transfer Protocol Secure (HTTPS) instead of Transport Layer Security (TLS) as its communication protocol. This is a protocol for secure communication over a computer network. The protocol ensures that no data is modified during transmission.

TLS is a cryptographic protocol of HTTPS that provides communication security over a computer network. The TLS protocol aims primarily to provide privacy and data integrity between two communicating computer applications. The TLS configuration follows the latest security recommendations for strong encryption.

---

## 7 Application-Specific Virus Scan

SAP Sports One provides a virus scanner to prevent manipulated or malicious files from damaging the system.

In addition to the virus scanner, SAP Sports One has implemented a combination of whitelist and blacklist patterns to prevent uploading of file types, which might include and execute malicious software code on a system.

The whitelist defines the file types by MIME type pattern, which can be uploaded into the system: For example:

MIME type: `image/*`

to allow the file upload of all images.

The blacklist defines the explicit file types by MIME type pattern, which cannot be uploaded: For example:

MIME type: `image/svg+xml`

to prevent the file upload of scalable vector graphics, which might contain malicious software code.

Both the whitelist and the blacklist are maintained by SAP.

## 8 Data Storage Security

### Data base encryption

SAP Sport One uses SAP HANA database as data storage. During system installation, the database is enabled for encryption and the data is encrypted. It is possible to check the encryption state within the SAP Sports One Web Application.

#### Tools

Tool	Detailed Description	Prerequisites
<a href="#">Security Settings</a> <a href="#">Data Security</a> → <a href="#">Security Settings</a>   <a href="#">Database Encryption</a>	Check the database encryption state.	<a href="#">Data Security Officer Role</a> within <a href="#">SAP Sports One</a>

### Mobile Device Storage

For SAP Sports One Mobile Applications, the offline storage is additionally encrypted using the device and OS capabilities. If the user decides not to use encryption for the mobile device, then the applications do not start.

## 9 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 about 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 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

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person (“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.
Purpose	A legal, contractual, or other 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.
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Deletion	The irreversible destruction of personal data.
Retention period	The period of time between the end of purpose (EoP) for a data set and when the data set is deleted, subject to applicable laws. It is a combination of the residence period and the blocking period.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the EoP has been reached, the data is blocked and can be accessed only by users with special authorization.
Sensitive personal data	A category of personal data that usually includes the following type of information: <ul style="list-style-type: none"><li>○ Special categories of personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,</li></ul>

Term	Definition
	<p>and the processing of genetic data, biometric data, data concerning health or sex life or sexual orientation</p> <ul style="list-style-type: none"> <li>○ Personal data subject to professional secrecy</li> <li>○ Personal data relating to criminal or administrative offences</li> <li>○ Personal data concerning insurances, bank, or credit card accounts</li> </ul>
Consent	The action of the data subject confirming that the use of their personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOMs). The following topics are related to data protection and require appropriate TOMs:

- Access control: Authentication features as described in section [User Administration, Authentication, and Authorization \[Page 12\]](#).
- Authorizations: Authorization concept as described in section [User Administration, Authentication, and Authorization \[Page 12\]](#).
- Read access logging and Change access logging: as described in section [Read Access Logging and Change Access Logging \[Page 22\]](#).
- Communication security: as described in section [Network and Communication Security \[Page 17\]](#).
- Availability control as described in section [Data Storage Security \[Page 19\]](#)
- Separation by purpose: Is subject to the organizational model implemented and must be applied as part of the authorization concept.

#### Configuration of Data Protection Functions

Certain central functions that support data protection compliance are available within SAP Sports One Web Applications under the [Data Security](#) menu entry (the Data Security Officer role is required).

## 9.1 Deletion of Personal Data

SAP Sports One might process personal data that is subject to the data protection laws applicable in specific countries as described in SAP Note 1825544.

Retention, blocking, and deletion of data can be defined individually for several SAP Sports One objects.

#### Tools

Tool	Detailed Description	Prerequisites
<a href="#">Retention Policies</a> <a href="#">Data Security</a> → <a href="#">Retention Policies</a>	Activate retention policies, and define blocking and deletion periods.	<a href="#">Data Security Officer Role</a> within <a href="#">SAP Sports One</a>

Tool	Detailed Description	Prerequisites
<a href="#">Retention Policies</a> <a href="#">Data Security → Retention Policies</a>	View blocked data and unblock data records.	<a href="#">Data Security Officer Role</a> within <a href="#">SAP Sports One</a>

In this tool, the Data Security Officer can enable the retention policy for several SAP Sports One objects.

If the policy is active, the Data Security Officer must define the period where the object is actively used and actively available in the system (field: blocked after .. days).

When this period is over, that is, the end of the purpose is reached, the object is blocked.

The object is in the blocked state if a retention period is applicable.

Blocking of data prevents SAP Sports One business users from displaying and using data that may include personal data and data that is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- Display: The system does not display blocked data.
- Search: It is not possible to search for blocked data or to search for a business object using blocked data in the search criteria.
- Analytics: SAP Analytics Cloud does not use blocked data.

Additionally, it is required to enter the period after which the object is physically deleted from the system (field: deleted after ... days).

If the policy is not active, the object persists in the system if it is not deleted.

Switching off a policy will not automatically unblock objects.

## 9.2 Read Access Logging and Change Access Logging

Read access and change access to personal data is partially based on legislation, and it is subject to logging functionality. The [Access Log](#) component of SAP Sports One can be used to monitor and log access to data and provide information such as which business users accessed personal data and when they did so.

Tools

Tool	Detailed Description	Prerequisites
<a href="#">Access Log</a> <a href="#">Data Security → Access Log</a>	Activate read access and change access logging, and view the log details	<a href="#">Data Security Officer Role</a> within <a href="#">SAP Sports One</a>

### Note

Before you enable the access log, you must define a deletion period under Retention Policies for the object Access Log.

The Data Security Officer can define which database objects are relevant for access logging. SAP Sports One provides the following configuration for:

- Customizing Data
  - Change access logging
  - No logging
- Master Data and Transactional Data
  - Read access logging
  - Change access logging
  - Read access and change access logging
  - No logging

The access log detailed report can be filtered and presents the timestamp, user, action, status, and statement of the access.

## 9.3 Personal Data Report

In accordance with legislations on data privacy and informational self-determination, which are subject to national regulations, any individual is entitled to request the disclosure of their personal data stored in the system. A report collects all relevant data, arranges it in meaningful content sections, and provides it as a download.

Tools

Tool	Detailed Description	Prerequisites
<a href="#">Personal Data</a> <a href="#">Data Security → Personal Data</a>	Search for a person and create a PDF document with data stored related to this person	<a href="#">Data Security Officer Role</a> within <a href="#">SAP Sports One</a>

SAP Sports One provides the ability to search for a person in the Web Application and generate PDF documents related to this person, with corresponding data.

# 10 Consent Management

SAP Sports One offers a flexible consent management tool to get the acceptance of an uploaded consent document from special user groups or from all Web Application users.

## Tools

Tool	Detailed Description	Prerequisites
<a href="#">Consent Management</a> <a href="#">Data Security → Terms of Use</a>	Upload consent documents optional for user groups, mobile apps, and validity and track acceptance.	<a href="#">Data Security Officer Role</a> within <a href="#">SAP Sports One</a>
<a href="#">Revoke User Consent</a> <a href="#">Own Settings → My User Consent</a>	Display user consent with Terms of Use document. Revoke user consent.	<a href="#">User in SAP Sports One</a>

If a document is active and within the validity period, each Web Application user is prompted with the consent document after they login and until they accept the document. If a user rejects the document, they are automatically logged out.

Each user can display the granted user consent with the corresponding Terms of Use document. They can also revoke the user consent within the validity range of the document.

For each mobile app (SAP Team One, SAP Challenger Insights, SAP Scout One) a user consent document (in plain text) may also be provided, which then must be accepted from within the mobile app. Or, in the case of SAP Team One, it may be accepted either in the Web Application or the mobile app.





[www.sap.com/contactsap](http://www.sap.com/contactsap)



© 2016 SAP SE or an SAP affiliate company. All rights reserved.  
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Please see <http://www.sap.com/corporate-en/about/legal/copyright/index.html> for additional trademark information and notices.

Material Number: NA

**SAP**