tts performance suite

DATA PROTECTION DECLARATION

31.01.2024

Note

This document aims to highlight to the user potential interfaces to the most recent data protection issues. The information included in this document reflects the current perspective of tts at the time of publication.

Table of contents

1 Name and address of the person responsible

The person responsible in accordance with the General Data Protection Regulation and other national data protection laws of the member states, as well as other data protection regulations, is the company that deploys tt performance suite (hereafter referred to as the "company").

2 Name and address of the data protection officer

The data protection officer of the tts Group:
Liv Ponce Ortiz
Data Protection & Compliance
Tel: +49 6221 894690
Email: dsb@tt-s.com

3 General information about data processing

When using tts performance suite, the personal data of users are only processed to the extent that this is necessary for using the software.

Data processing is based on the consent of users. The legal basis is Art. 6 para. 1 lit. a of the EU General Data Protection Regulation (GDPR). The user must declare his/her consent at any time to the company in the form of a corresponding declaration to the company.

The personal data of the person in question will be deleted or blocked as soon as the purpose of storage no longer applies. In addition, data may also be stored if this has been provided for by the European or national legislator in EU regulations, laws or other provisions to which the person responsible is subject. The data will also be blocked or deleted if a storage period prescribed by the aforementioned standards expires, unless there is a necessity for continued storage of the data for the conclusion or fulfillment of a contract.

4 Rechte des Nutzers als betroffene Person

The user has the following rights with regard to the personal data concerning him/her vis-à-vis the company:

- right of information,
- right of rectification or deletion,
- right of restriction of processing,
- right of object to processing,
- right of data portability.

The user also has the right to complain to a data protection supervisory body about the processing of his/her personal data by the company.

5 Data processing by tts GmbH

tts performance suite is operated by tts GmbH Schneidmühlstraße 19, 69115 Heidelberg, Germany (www.tt-s.com, hereafter referred to as "tts"). The user's personal data are processed by tts in accordance with the terms of the contract with the company regarding the use of tts performance suite and in order to facilitate its use.

The contractual agreements between tts and the company comply with the legal requirements for data processing by external service providers.

6 Data processing by hosting service providers

tts performance suite is hosted on servers belonging to external hosting service providers. The hosting service providers therefore have potential access to users' personal data.

tts has concluded a data protection agreement with the hosting service providers which complies with the legal requirements.

The processing of personal data shall take place exclusively in the territory of the Federal Republic of Germany, in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior documented instruction of the Customer (Art. 28 (3) lit. a GDPR) and may only take place if the special requirements of Art. 44-49 GDPR are met.

7 Technical information on data protection

tts does not save any user-specific data from the tts performance suite Web Publisher or QuickAccess, from the tts performance suite Workbench or from the tts performance suite Client.

No personal data are transferred to tts, either automatically or via an automated query.

Insofar as tts has identified programs as products from upstream suppliers or third-party providers, tts only vouches for their properties to the extent that they are essential for the use of the application programs from tts. Furthermore, tts does not vouch for the information in the product descriptions of the respective manufacturers.

7.1 Storage of end-user and author data

In the case of end users, user master records are only required whenever the personalization functions of the tts performance suite Web Publisher or QuickAccess are activated.

Among other things, this form of personalization facilitates the display of documentation to users that is appropriate for their role within the company. If personalization has been deactivated, all users have access to the same content, but role filtering is still possible via manual filtering.

User master records have to be created and saved to facilitate the use of the authoring functions within the tts performance suite Workbench and the tts performance suite Client.

The following data are transmitted (i.e. saved on the server) when the personalization function is activated and the tts performance suite Workbench and tts performance suite Client are used:

- **Login data**
  The username and password are saved in the system to facilitate logging on to the tts performance suite Web Publisher or QuickAccess or to the tts performance suite Workbench. The username can be chosen freely and the anonymization of all user-bound data can be ensured by using pseudonyms. Just a few special functions, which needless to say require information regarding the user, cannot be used when using anonymized user data (e.g. the e-mail notifying an author of a document's status change or the web portal's personalization functions for end users).
    - **LDAP-based login data**
      The tts performance suite Web Publisher and the tts performance suite Workbench save the unique User ID imported from the Active Directory server. The password is not saved in this case because it is directly verified by the actual Active Directory server.

- **Storage in the OTP cache**
  One-Time Passwords (OTP), which are valid for a short term, are generated to protect end-users' access via the tts performance suite Web Publisher and QuickAccess. Whenever an OTP is requested for a user, his/her login, profile UUID, roles and license are stored in the OTP cache. These data are invalidated by the cache when the set period expires and are subsequently deleted.

- **Personal information**
  In cases where personal information is entered by users themselves or an administrator, it may be stored within the tts performance suite Workbench. This does not involve checking the validity of the data, meaning that these data can also be fictional. The specification of a valid and therefore traceable e-mail address is up to the user or administrator and may result in the above-mentioned usage restrictions.

- **LDAP-based information**
  Whenever an Active Directory server is used for user administration, personal information in the form of family name, first name and e-mail address can be read-out from the Active Directory

User master records	Mandatory
Username and password (if maintained in the system, can alternatively be checked against an external directory system)	✓
License assignment (assigns the user to a pool of available licenses)	✓
Sprache (für Benutzeroberfläche und Anzeige von Inhalten and display of content)	✓
First and family name	-
E-mail address (used for Workflow notifications)	-
Author roles (e.g. "e-learning author" or "translator")	-
Process roles (e.g. "purchaser"; primarily used for end users in cases where portal personalization is desired)	-
Display size of system dialog windows	-

- **Server-side log files**
  In the standard minimal configuration, the login and logout of end users / authors, as well as actions performed on objects (such as the checking-in and checking-out of objects), along with the user identity are all recorded server-side and stored in the log files. Logging can be modified by the administrator. Data are stored in the Access Log on the superordinate web server (TomCat), where they are beyond the reach of tts.

- **Versioning**
  If versioning is activated, the changes made by users are also saved with the versions and can be viewed via a versioning protocol. No user information is saved in this protocol. This also applies to the changes made to the previous versions of the current document.

- **Retention period of stored data**
  Stored object-based data, which are also visible to the authors in the GUI, are removed upon deleting the respective object.

- **Time of login/logout**
  The time of a user's last login and logout is saved.

- **Search index**
  Solr is used for the search function in tts performance suite. Data are therefore not only saved in the database of the Workbench but also in the Solr index. Only the internal user profile IDs are stored in the Owner and Assignee fields, and their assignment is untraceable for outside sources without access to the database. Plain text, usually consisting of the family name and first name from the user profile, is

stored in the Author field (custom property). The login name is saved if these are not available. The Technical information on data protection Page 8 of 8 same data protection aspects as those used for displaying the change history also apply here.

- **Object-related data storage**
  When editing objects within the tts performance suite Workbench, object-based changes are transmitted to the server, where they are stored accordingly. The changes made are stored in the object's protocol, in combination with the username, and can be viewed by other users via the GUI.

Data type	
Change to an object	Changes made to the parameters or content of the objects.
Date and time of the change	Date and time of an object change. The time at which changes are made to objects is saved.
Username	The username for identifying the user doing the editing.

7.2 Communication between server and client

Communication between the client and server is carried out in an unencrypted manner via HTTP. We therefore strongly recommend using HTTPS to ensure the encrypted transmission of data. The use of our SaaS offer is exclusively restricted to encrypted HTTPS.

7.3 Data storage in the tts performance force client

In the standard configuration, the tts knowledge force client stores personal settings, such as view settings and modified program settings, in the personal profile directory on the local drive of the corresponding authors. The passwords used are also encrypted and stored by default.

8 Activation of AI functions (optional)

As part of the use of the tts performance suite, various AI functions can be activated as a beta version at the customer's request. Which AI functions are activated is defined in the " Additional agreement for the Order Form - activation of AI function(s)".

To activate the AI functions via the tts performance suite, the customer must provide tts with the corresponding API key of the AI provider with which the tts performance suite is to be connected via API. Then tts stores this API key in the server-side configuration files of the tts performance suite to be able to establish the connection to the AI function(s).

It is expressly pointed out that the AI providers cannot access any personal data from the tts performance suite, and that personal data will not be passed on to the AI providers.

The data protection provisions and terms of use of the AI providers apply.