Scheer IMC

LMS Settings for Data Protection and Security

Project Guide

imc Learning Suite | Consulting Department | September 29, 2025

Content

Scheer IMC
information multimedia communication AG

Scheer Tower, Uni-Campus Nord
66123 Saarbrücken
Germany

Phone +49 681 9476-0
Fax +49 681 9476-530
info@im-c.com
scheer-imc.com

1 Information

The purpose of this guide is to assist our customers with data protection and security settings as part of an LMS implementation project. This guide contains the most important information on setting options in these two areas, which should be considered as part of the implementation project.

Reference is made to the additional official documents provided by the standard product imc Learning Suite, which can be accessed by customers. This guide therefore does not provide a complete documentation of all possibilities and measures of the standard product. Rather, it covers the most important setting options that need to be considered in the context of an implementation project.

Decisions and settings should be recorded on all topics covered in this client guide as part of the project closure procedure. The following areas are explained below:

1.1 Privacy policy

The LMS allows the use of a privacy policy as part of the login process. The data protection declaration can be activated or deactivated (usually per client).

If the privacy policy is active, the user must accept the privacy policy during the first login process. Even if changes are made to the text of the privacy policy statement, the learner must accept the new statement within next login process. A declination of the privacy policy will result in the user being deactivated.

In addition, it is possible to give the learner the option to actively decline the privacy policy in the system, which also results in the deactivation of his user account.

In the implementation project, it must be defined and configured whether the privacy policy is used and, if so, whether declining the statement is permitted at a later stage.

1.2 Deletion concept

The LMS allows the automatic deletion (physical deletion or anonymisation) of user accounts, e.g., to fulfil retention periods. In addition, manual deletion of user objects is possible at any time by an administrator. The LMS also offers the option for users to delete their account themselves, which also results in a direct physical deletion or anonymisation of the user object. Alternatively, users must send a deletion request by email and outside the LMS to the administration of the LMS.

In the implementation project, it must be defined and configured whether users are allowed to delete their account themselves (or whether they can only send a deletion request by e-mail to the administration) and whether there are automated deletion routines that physically delete or anonymise user objects.

1.3 Security settings

The LMS is initialised with security settings by default (*security by default*). However, there are reasons to reduce security settings for specific scenarios:

- If an external catalogue (offers before user login) is used, the setting "force login" must be deactivated. In addition, the call of course description pages must be activated so that it is also possible to call objects for which access by the portal client is permitted (object releases) before login.
- When saving description fields and text fields, HTML content is checked and removed by default. This can lead to content being modified after saving. A temporary deactivation of this security feature is possible; a permanent deactivation should be carefully considered.

In the implementation project, it must be defined and configured whether security settings have been adapted compared to the security by default approach and for what purpose this has been done.

1.4 Authentication

The LMS supports various authentication procedures (including local logon, SSO via SAML2 or OIDC), which can be set per client. Access to client-specific portal pages can be implemented via own URLs or via parameters (*client*). For local login via the LMS, specific password policies can be defined that deviate from the standard configuration. This concerns the password complexity, the duration of password validity, the options for generating passwords and, if applicable, the use of a 2FA procedure. In addition, it must be considered whether authentication procedures must be configured in an environment-specific manner. This is particularly necessary for SSO procedures, as a productive environment and a test environment require different return points for the SSO procedure.

In the implementation project, it must be defined and configured which authentication procedures (client-specific and environment-specific, if applicable) are set up and whether there have been changes to the password guidelines for local logon.

1.5 Anonymisation scripts

If the customer operates other environments in addition to the productive environment (*test*, *stage*, *dev* or similar), imc recommends mirroring the productive data in the other environments from time to time. This ensures that the data is comparable, and a real test possibility is maintained. The mirroring of the data always includes the complete data, i.e., the database including the objects and the configuration as well as the stored files in the file directory of the LMS. Partial mirroring is not possible.

If the LMS is operated by imc in the cloud, imc will anonymise user data to comply with the EU-GDPR. It is possible to exclude users from anonymisation to enable testing in non-productive environments. Which user accounts are to be excluded from anonymisation is determined by the customer in the project. For this purpose, it is recommended to create groups in the LMS and to exclude their users from anonymisation.

If the customer does the LMS operation without imc (on-premises, in contrast to cloud operation by imc), it is important to clarify the transfer of a possibly anonymised database to imc for support purposes as part of the implementation project. The database should be transferred in the same way as imc provides new delivery packages (via SFTP).

In the implementation project, it must be defined and configured which users or user groups are to be excluded from anonymisation if other environments (e.g., test environment) are existing in addition to the productive environment. It must also be ensured that a database can be transferred to imc for support purposes in the case of on-premises operation.