

imc Learning Suite in the context of data protection

imc Learning Suite in the context of data protection

Author(s): Lia Ghiță, Dr. Peter Zönnchen

Date: 2022-01-18

Document	Description
Version	ILS 14.11
Status (Draft / Review / Finalisation)	Finalisation
Contact Person(s)	Product Management Team

History	Status	Who
2018-04-12	Draft	Lia Ghiță
2021-02-15	Review	Andreas Pohl
2021-12-07	Review	Lia Ghiță
2022-01-18	Finalisation	Dr. Peter Zönnchen

Content

1	Introduction	4
2	The right to be forgotten	5
2.1	imc Learning Suite	5
2.2	imc Learning Portal	9
2.3	imc Learning Apps	10
3	Easier access to one's data	10
4	The right to data portability	12
5	Consent for use of cookies	14
6	Processes and system configuration	15
7	Special considerations	16

1 Introduction

Data protection has always been an important aspect of all imc products and imc always strives for the highest possible data protection standards.

The European Commission put forward its [EU Data Protection Reform](#) in January 2012 to make Europe fit for the digital age. The Regulation will apply from 25 May 2018.

imc has responded by thoroughly reviewing the new data protection regulation requirements and improving our products where necessary to support compliance. As such our customers are assured that, with respect to imc products, they are fully prepared to be compliant when regulation comes into force.

The main regulatory requirements are outlined in brief as follows. Further details on each can be found in the subsequent chapters.

The right to be forgotten

When an individual no longer wants her/his data to be processed and there are no legitimate grounds for retaining it the data can be deleted. This is about protecting the privacy of individuals, not about erasing past events or restricting freedom of the press. This aspect is reflected in the imc products by allowing the user to request the deletion of the data from the system as well as the possibility for an administrator to remove a user from the back-end.

Easier access to one's data

Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. A right to data portability will make it easier for individuals to transfer personal data between service providers. The Learning Suite provides the option for the learner to request a copy of their personal data.

Additionally, aspects that must be integrated in imc's processes cover the following.

The right to know when one's data has been hacked

Companies and organizations must notify the national supervisory authority of data breaches which put individuals at risk and communicate to the data subject all high-risk breaches as soon as possible so that users can take appropriate measures.

Data protection by design and by default

'Data protection by design' and 'Data protection by default' are now essential elements in EU data protection rules. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.

This is an extract from the EU regulation. For imc this means that with every new implementation we add to the system we are considering whether any new personal data will be involved, such that we include it in the deletion process and the export of personal data.

2 The right to be forgotten

2.1 imc Learning Suite

imc Learning Suite provides users with the possibility to request the deletion of their personal data. This option can be configured whether to be shown or not in the navigation. The deletion of a user can also be triggered by an administrator from the backend.

The Learning Suite will provide two levels of deletion:

- **Anonymization of user data**
scrambles all personal data and will generate new random IDs for the users (Pseudonymisation).
- **Full deletion**
completely deletes the user record. By enabling this option, the learning history will be lost for the deleted user.

When the data deletion process is triggered, the following data will be ALWAYS removed from the system:

Development plans, Guestbook, Chats, Address book, User profile, Gamification: Experience tracks and badges, Job profiles and skills, Personal notifications, Saved search profiles, column settings in search, Favourites, Resource management assignments, Report favourites, Report subscriptions, Positions, Votes submitted in surveys, Personal appointments, Who is online.

We have thoroughly analysed the nature of the data we collect and assessed whether or not it can be considered personal data. No additional personal data should remain in the system after it has been deleted.

The following data will be removed only if full deletion is active:

Learning history, test results and feedback results

When the anonymization type of deletion is used, the learning history will be available in reports but the user can no longer be identified, as the user ID is anonymized. When the full deletion is selected, then all the data is deleted, including the learning history.

In the following contexts, learner contributions themselves will not be removed, but the learner will be shown as a “deleted user”:

Forums, Pin board, Wiki, Document archive, Accounts created via LMS on external systems such as Mahara, GoToMeeting/GoToWebinar, LTI, Adobe meetings.

Content can only be deleted manually by an administrator. The user who requests the deletion of his account will not be able to choose to delete content as well.

The following particular considerations and advice applies:

- The user's contributions on social media belongs to the community and will not be removed.
- The user is responsible for not providing personal information inside comments or posts.
- The customer is responsible for the management of accounts created on external systems.

These aspects will be described and included in the default privacy policy of the LMS.

The following data contained in the system's data folder will be removed as part of the deletion process when a user deletion request is registered (imc Learning Suite data folder contents):

person - personimport – csv

group – groupimport

profile picture of the user

competence

course - logs

serialletter

position – positionimport

assignmentimport

osreport – subscriptions

dbarchive - internal and system messages.

The following related considerations and advice applies:

- Please consider permanent storage in case you want to ensure that this data is not lost.
- In addition, please ensure that deleted users are no longer included in a leading user directory (e.g. LDAP/Active directory).

Additional configuration possibilities

To support our customers in maintaining data needed for compliance with other regulations, the Learning Suite will provide the possibility to define a time frame in months, based on which the data will be kept in the system while the user is set to passive.

Either the deletion is carried through immediately, or the customer can choose to delay it. This is merely a configuration and up to the customer to enable a delay, else by default the most restrictive option will be used -> immediate deletion.

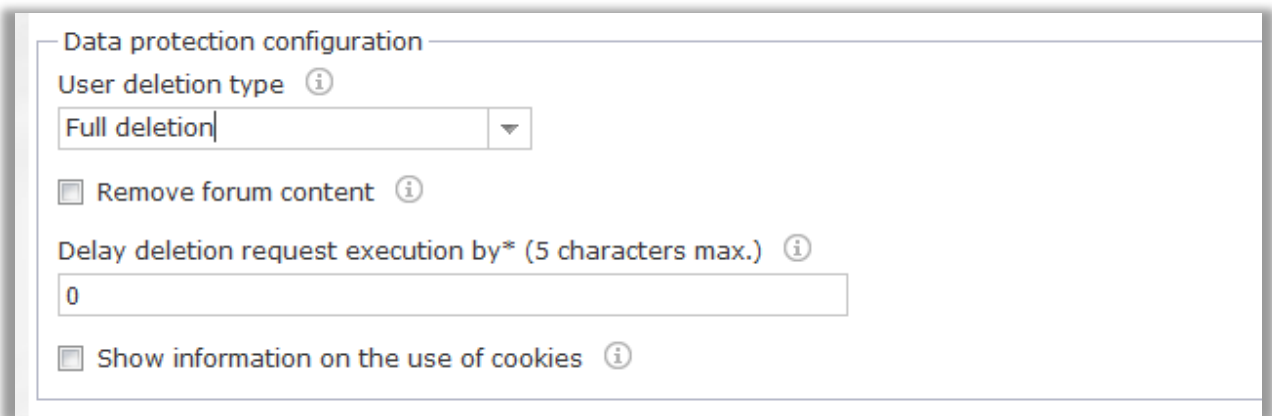
The settings related to the type of deletion and removal of forum content will take effect when the deletion job runs.

Hint to consultants:

You can configure the deletion job to run after the person import job, to avoid skipping imports.

The setting is available at the Client Functionalities and Setting tab.

One additional configuration is introduced in the same section, that allows the customer to specify if the forum posts and replies should be included in the anonymization/deletion process. As a consequence, the contents of such posts will be lost.



Data protection configuration

User deletion type ⓘ

Full deletion ▼

☐ Remove forum content ⓘ

Delay deletion request execution by* (5 characters max.) ⓘ

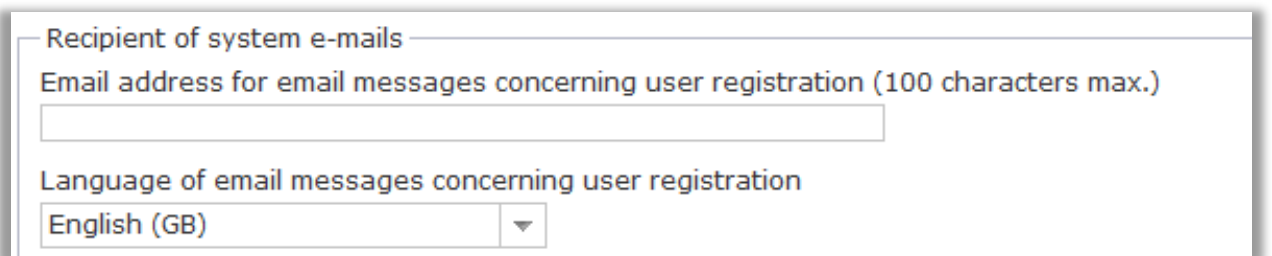
0

☐ Show information on the use of cookies ⓘ

Fig. 2.1: Client Management, Section „Data protection configuration“

Additional considerations

Whenever a user requests the deletion of their own account, an e-mail will be sent to the person responsible with registrations. At client level such an e-mail address can be defined, otherwise the e-mail address defined in the businessprocess.xml for the same role will be used.



Recipient of system e-mails

Email address for email messages concerning user registration (100 characters max.)

Language of email messages concerning user registration

English (GB) ▼

Fig. 2.2: Client Management, Section „Recipient of system e-mails“

The e-mail will inform that the deletion was requested by the user, also mentioning the need that the responsible person takes care of informing external systems about the user deletion, if needed.

The alert displayed when deleting a user from the backend is also enhanced with this message.

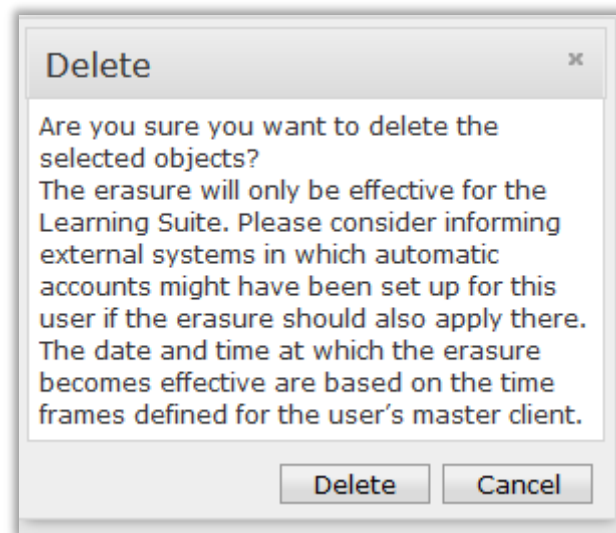


Fig. 2.3: Dialog "Delete"

Proof of deletion

Whenever the deletion process for a particular user is started in the system, a log entry will be provided confirming the start of the process. An additional log entry is provided at the time when the process is completed.

The log entry can be located by using the ID that used to belong to the deleted user.

Handling of failed deletions

It could be possible that the deletion process cannot be finalized. In such a case, the changes are rolled back and the responsible person is informed via e-mail of the need to restart the deletion process from the back-end.

2.2 imc Learning Portal

Users can request the deletion of their account via the imc Learning Portal as well.

When requesting the deletion, the user is asked to confirm his password (for both local and LDAP authentication) as an extra security measure.

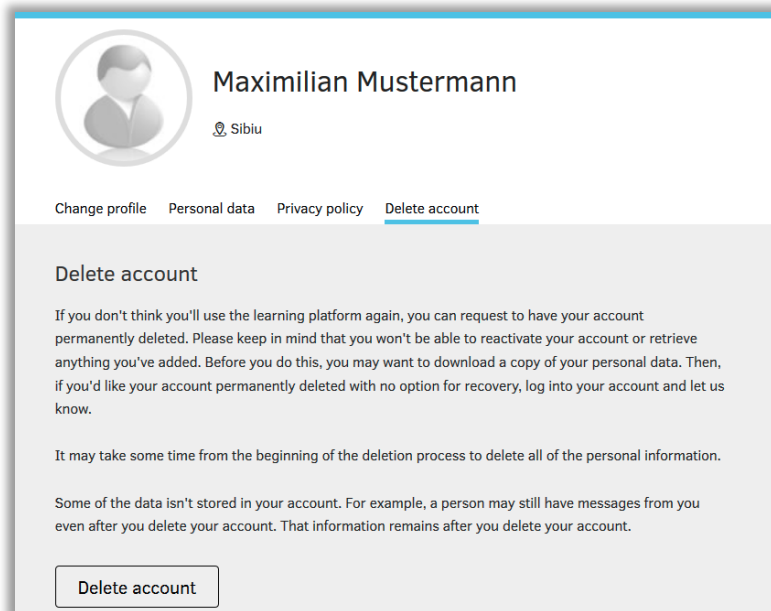


Fig. 2.4: Dialog "Delete account"

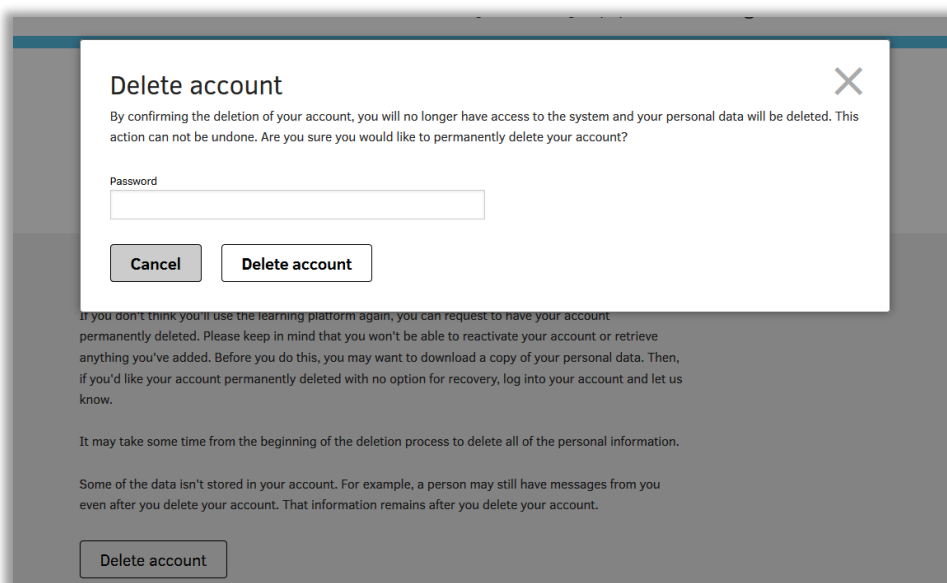


Fig. 2.5: Confirm "Delete account"

2.3 imc Learning Apps

The mobile apps and the Windows Learning App do not provide the possibility for the user to request the account deletion.

3 Easier access to one's data




With its privacy policy, imc Learning Suite provides detailed information on how data is processed in the context of learning management done in the system. The privacy policy can be included into the first login and when activated must be confirmed as a mandatory step to allow continuous use of the system.


Privacy policies can be configured differently for each client. A system function to review and withdraw consent later is also available by configuration.


The privacy policy can be further adapted by the customer to match their concrete scenario and usage of personal data.

This functionality is available in imc Learning Suite, imc Learning Portal and the Mobile Apps. Now, the Windows app requires users to login first at the Learning Suite before logging in on the app.



[Catalogs](#)
[Login](#)
[Sign up](#)


Accept privacy policy


Update profile

Accept privacy policy

Please accept the privacy policy to proceed.

In accordance with article 13, paragraphs 1 and 2 of the EU Data Protection Regulation we inform you below about the collection, processing and use of your personal data in connection with the use of this digital learning platform.

On this digital learning platform we invite you to our web-based training programs. In order to assign a selected tutorial to you and provide you with the required login information, we need to process some of your personal information in our login form.

If, for example, you are an employee or customer in a contractual relationship with us, or if your personal data is provided to us here as part of a business initiation, or if necessary also updated, we process this personal data for the implementation of the contractual relationship or for pre-contractual purposes at your request (Art 6 Para. 1 b) GDPR).

You may also have other reasons for entering your data here. As far as we collect your personal data (e.g. name, surname, address or e-mail address, place of birth or date of birth) via this digital learning platform, this is always on a voluntary basis.

The following information is stored in the learning platform:

Image, Title, Academic title, First name, Last name, Email, Number, Position, Country, Company, Title of supervisor, First name of

All registered users have access to these data:

The user help desk also has access to the following data:

City, Department, Gender, Preferred working language, Change password with next login, Changing risk, Travel willingness, Login name, Password, Type of authentication, Show who is online, Send info email, User time zone, Forward internal email to an external address, Show notification upon receipt of new high-priority messages, Show notification upon receipt of new messages, Exclude as mail recipient, Send administrator message, Allow proxy enrollment, Authentication status, Cost center, CSV ID, LDAP ID, ERP ID, ERP System ID, Type of deregistration, Registered until (target date)

Your personal data may be transferred to service providers who necessarily support us for the purpose of maintenance and support of the digital learning platform.

Since our group of companies also includes companies in third countries (e.g. Australia) or, in order to be competitive, also support service providers with company headquarters, group parent or data centre in third countries, it may be necessary for this to be passed on. In such cases we ensure that only those data are accessed which are necessary for the performance of the specific task and that appropriate security measures (e.g. adequacy resolution of the EU Commission, standard contractual clauses) have been taken.

If you do not request deletion of the data, the data will be stored by us as long as they are needed for the purpose for which they were collected. In addition, especially if a contractual relationship exists or existed, the data may be stored for the fulfilment of commercial and tax storage obligations (e.g. 2 to 10 years) or to preserve evidence within the framework of statutory statute of limitations (e.g. up to 30 years).

Content provided as part of social media and community, such as forums, wikis, exercises, pinboards, etc will not be deleted.

Please ensure to not provide your personal information in such contexts.

Within the framework of the statutory provisions, you have many rights in the processing of your personal data: Right to information, right to correction, right to cancellation, right to limitation of processing and right to data transferability. There are restrictions on the right to information and deletion, for example in accordance with § 34 and 35 BDSG.

If we process your data to protect legitimate interests, you may object to such processing if your particular situation gives rise to reasons against data processing.

You have the right to complain to a competent data protection supervisory authority. Providing your personal data (see above) is a necessary prerequisite for you to be able to inform yourself about our courses on the digital learning platform, enrol and complete the courses. At the same time it is necessary for us to provide you with the login data.

I agree to the editing of data according to the explanation given above.

Decline privacy policy

Accept privacy policy

Imprint

Terms of use

[Deutsch](#)
[English \(US\)](#)
[English \(UK\)](#)
[Español](#)
[Français](#)
[Italiano](#)

Fig. 3.1: Accept privacy policy

4 The right to data portability

Regarding the data portability, imc Learning Suite provides users with the possibility to request a personal data report which will be delivered via e-mail.

The report contains the following data:

Development plans, Group assignment, Guestbook, Forums, Chats, Pin board, Wikis, Address book, User profile, Votes submitted in surveys, Job profiles and skills, Comments on competencies, Personal notifications, Saved search profiles, column settings in search, Favourites, Resource management of persons, Positions, Assessments, Test and feedback results, SCO status in courses and catalogues, AU status in courses and catalogues, OJT: Results of the training module, Personal appointments, Course, course template and programme progress and history, Media completion in the catalogue, Gamification: Experience tracks and badges

Dr. Maximilian Mustermann				
Skills				
name	level_1	level_2	confirmation_status	schedule_date
MS Excel	99	0	Unknown	01-Feb-2018
MS Word	100	0	Unknown	
MS PowerPoint	99	49	Unknown	29-Jan-2018
Information Security Compliance	0	0	Confirmed	
Managing Risk	0	0	Unknown	
Rhetoric	0	75	Confirmed	
Project Management	80	33	Unknown	
Core Project Management skills	0	0	Unknown	
- Advanced Health & safety	0	100	Confirmed	06-Feb-2018
- COSHH	49	0	Unknown	
- Equality & Diversity	0	100	Confirmed	
- Information governance	0	0	Unknown	
- MHA and Legal frameworks	0	0	Unknown	
Employee development	50	0	Unknown	
Business orientation	66	0	Unknown	
Advertising (OpenScout 3.1)	0	0	Unknown	
Identify and counter money laundering	99	0	Unknown	
Excel DD TEST	79	0	Unknown	
Excel	100	0	Unknown	
Business English	49	100	Confirmed	24-Aug-2018
Business English	0	0	Unknown	

Fig. 4.1: Data report

In the imc Learning Portal, the navigation entry that allows the user to request the report is configurable from `navigation.xml`.

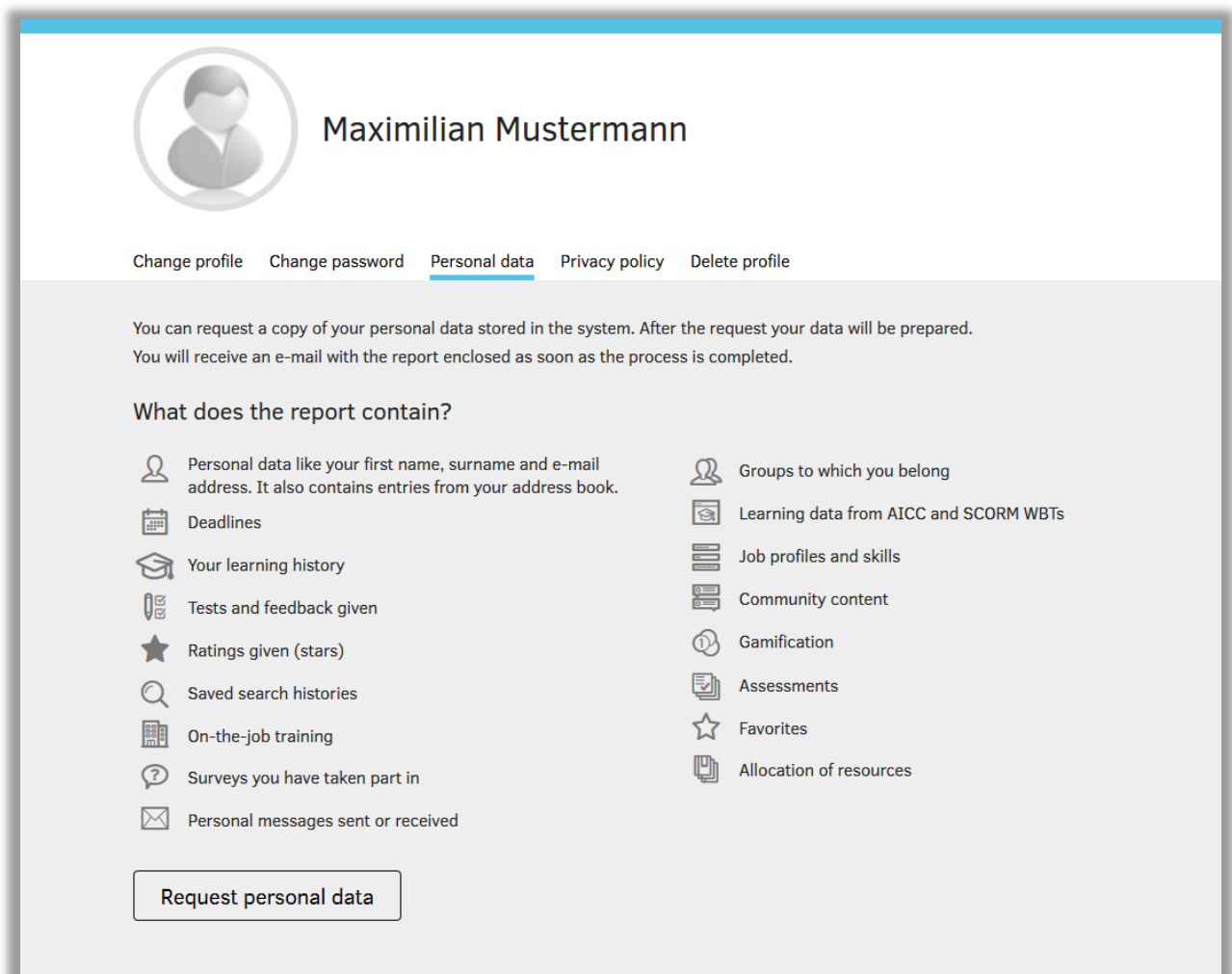


Fig. 4.2: Personal data

This functionality is available in the imc Learning Suite, imc Learning Portal and Mobile apps, but will not be available in the Desktop learning app.

5 Consent for use of cookies

imc Learning Portal will provide users with a notification about cookie usage upon the first access of the system via any related URL (if there is no cookie saved yet in the current browser settings). The Desktop app will be enhanced with this function in an upcoming release.

The cookie policy can be accessed via a URL linked to the notification. A system-wide default policy is defined and can be adjusted if needed.

There is no formal agreement needed. The agreement is considered to be granted when the user continues browsing.

The message will be displayed for as long as the user did not manually close it.

The notification is only shown in imc Learning Portal, as the imc Learning Suite does not use other cookies except strictly necessary cookies.

It can be configured at client level from the imc Learning Suite backend whether this notification will be shown to users or not in Learning Portal. The client parameter from the URL determines which client configuration is considered.

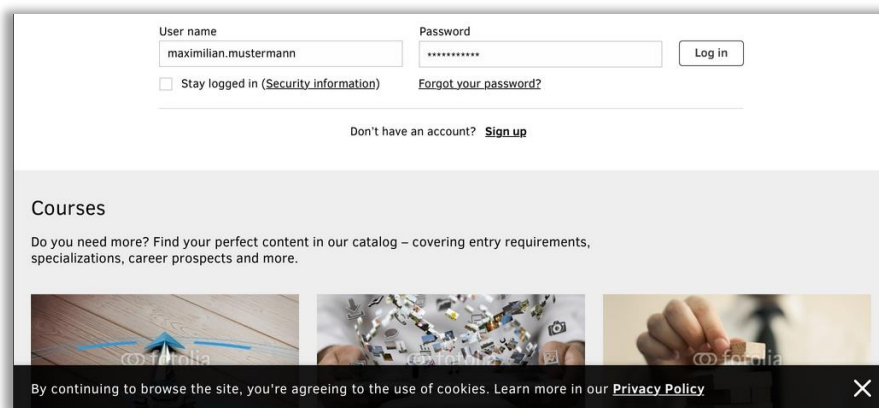


Fig. 5.1: Information about the use of cookies

6 Processes and system configuration

The following table contains all relevant settings for data protection compliance and where they can be activated from:

SETTING	Description	SCOPE
Privacy policy	Possibility to set up a policy that users need to agree with at the first login	Businessprocess.xml
Show cookie notice	The possibility to define if the cookie notification is shown	ILS client setting
Allow full deletion	Possibility to choose a deletion type	ILS client setting
Remove forum content	Possibility to choose whether forum content should also be removed when a user is removed from the system	ILS client setting
Show/Decline privacy policy	The display of the already agreed policy with the possibility to withdraw	navigation.xml/ILS navigation
Request personal data	The possibility to request a personal data report via mail	navigation.xml/ILS navigation
Delete account	The possibility to request the deletion of the account by the user	navigation.xml/ILS navigation

7 Special considerations



While ensuring that our products remain compliant with the General Data Protection Regulation, there are some aspects that cannot be controlled by product functionality and are in the customer's control. These aspects must be handled by each customer, according to their own processes.

User import

When deleting a user, the person import files will be deleted. However, the customer must ensure that the deleted user is also removed from any further imports.

External systems

As stated in the dedicated chapter, external systems need to be separately notified when the user data there should also be removed.

Privacy policy updates

imc will update the default privacy policy and provide this to customers, however we will not automatically update your policies since many of our customers have customized this to a high degree. Therefore, existing customers will need to plan to review and update as necessary the privacy policy to be in line with European data protection requirements.