Data Protection and Operational Security Information

V9.1

Imprint

evasys GmbH

Konrad-Zuse-Allee 13
21337 Lüneburg
Germany

Phone: +49 4131 7360 0
Telefax: +49 4131 7360 60
Email: info@evasys.de

Managing Directors: Silvio Ewert

USt-IdNr.: DE 179 384 158
Handelsregister: HRB-Nr. 1604, Lüneburg

Edited by Bernd Röver, Darin Schmälzlein

Table of Contents

A. Data Protection in evasys

1. Introduction

In this part of the document we describe the data protection aspects in operating Evasys. In this context, reference is made to the General Data Protection Regulation (GDPR) in the version promulgated on May 24th 2016), in force from May 25th 2018 with the Corrigendum (23 May 2018) to Regulation (EU) 2016/679 on data protection.

1.1. Definition of Terms

1.1.1. Product Variants

evasys for Higher Education

This is the evasys product variant in which university instructors and/or trainers have passive accounts at their disposal but cannot access these themselves. The administrator prepares all survey processes centrally and supervises the data processing. At the end of the survey period, the administrator can recall all of the data raised. Also, in central evaluation, instructor accounts can be activated, with which subsequent surveys can be carried out in a de-centralized form (see: User Types).

evasys for Neutral Language Use

Depending on the use case (course evaluation or general surveying), the system is configured to differing vocabulary concepts. For example, in the neutral language instructor or trainer accounts are called project accounts, or instead of courses we speak of topics. With regard to data protection however, both language variations are identical.

1.1.2. User Types

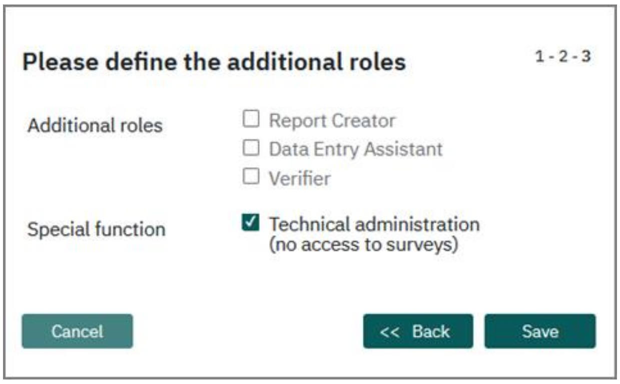
Administrator

Main user of the evasys system, responsible for the preparation, conducting and evaluation of survey waves (only central evaluation) and/or for the administration of user accounts (central and de-central evaluation).

The administrator can generate secondary administrators, for example for substitutes. Secondary administrators have the same access rights like the administrator but cannot create additional secondary administrators.

Technical Administrator

The technical administrator is a restricted version of the administrator without access to user, questionnaires, surveys, reports or raw data. This gives the IT department the possibility to configure system settings, interfaces and plug-ins without granting unnecessary access to surveys or personal data.



Please define the additional roles

1 - 2 - 3

Additional roles
□ Report Creator
□ Data Entry Assistant
□ Verifier

Special function
☑ Technical administration
(no access to surveys)

Figure 1: Technical administration

Subunit Administrator

Responsible for the preparation, conducting and evaluation of survey waves (only central evaluation) and/or for the administration of user accounts (central and de-central evaluation) of one or several specific subunits.

The administrator defines the subunits for each subunit administrator. The administrator can deactivate the subunit administrator’s access rights to survey results and/or the right to view scanned pages.

Active Instructor/Trainer or Project Account

Via the activated instructor/trainer/project account, surveys can be conducted, and the results recalled and evaluated.

The administrator can view the active user's surveys and results, as can a possible subunit administrator who has been assigned for this.

Report Creator

The report creator is a user created by the evasys administrator in order to produce summary reports for the captured data and to send comparative profile lines. The data access for each report creator can be defined

- for one subunit only,
- for subunit groups or
- system wide.

Data Entry Assistant

The data entry assistant is tasked with anonymizing the handwritten comments of participants in paper-based surveys, as far as the conducting organization deem this necessary. Several data entry assistants can work in parallel with the evasys web interface.

The administrator can limit access of the data entry assistant to one or more subunits.

The administrator can deactivate the data entry assistant's option to view the complete scanned questionnaire page.

Dean of Studies or Program Manager

The user operating this user profile can choose from a list of evaluated courses and make a selection, which is then individually compiled into a report.

Dean or Manager or Department Head

The user type dean/manager/department head differs compared to the user type instructor/trainer/project manager in that a complete utilization statistic for their specific subunit is displayed.

The user account can be switched to passive or active. An active dean/manager/department head, similar to the active instructor/trainer/project manager, can plan surveys, create questionnaires and, for example, access the activated QM screens (Phase 5).

With a passive account, the user only has access to the individually activated QM screens.

Verifier

The Verifier can be implemented for the visual correction of scanned sheets.

It checks the VividForms sheets processed by the VividForms reader and, where necessary, corrects the recognition. Verification can be switched on and off for surveys.

This can become necessary, because questionnaires filled out unclearly are not always correctly machine readable.

The verifier has access to all surveys and exams in the system which are set with verification. The administrator can restrict this access to one or several subunits.

The administrator can deactivate the verifier's option to view the complete scanned questionnaire page.

1.2. Web Service Settings

It is possible to manage users of SOAP API connections for external web services in “System Settings/Interfaces & Plug-ins”. The communication between evasys and external web services is encrypted by using the SSL protocol.

1.3. Guaranteeing Participant Anonymity

Evasys is furnished with numerous methodical measures, guaranteeing the anonymity of survey participants.

1.3.1. Paper based Surveys

The questionnaires templates are duplicated and identical for all survey participants. If a questionnaire contains more than one page, a numbering of the sections can be undertaken, so as to identify the single pages of a questionnaire in further processing.

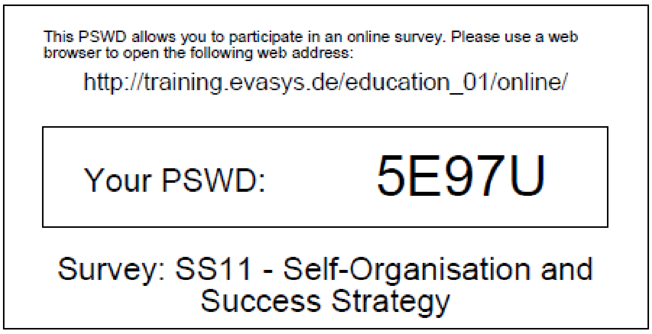
Please note: It may at times be possible to determine exactly the individual quire from the raw data when using continuous quire numeration; this is because the raw data contains the quire number. For this reason, surveys must be distributed anonymously or randomly, in order to guarantee anonymity.

During the scanning process, scans of the questionnaires are created and conveyed to the evasys software for evaluation of the readable zones (Checkboxes, Open Questions). The scans of the questionnaires can be filed for archiving purposes in a network directory controlled by the administrator. The archive file has to be defined in the Scanstation settings.

After extracting the raw data, these are available as pure binary information. The hand-written comments are extracted as graphics. With smaller survey groups, it may be necessary to anonymize these comments, protecting anonymity. To do this, evasys offers the user type “Data Entry Assistant” for anonymizing hand-written comments. If the survey group is relatively large, one may, under consideration of the substantial personnel requirement, waive an anonymization. This anonymization threshold sets a minimum number of returns under which survey responses are anonymized. The anonymization threshold can be adjusted individually.

1.3.2. Online Surveys

In evasys, the so called PSWD method is implemented for online surveys. All survey participants are issued an alpha-numeric code, giving access to the questionnaire.



This PSWD allows you to participate in an online survey. Please use a web browser to open the following web address:

http://training.evasys.de/education_01/online/

Your PSWD: 5E97U

Survey: SS11 - Self-Organisation and Success Strategy

Figure 2: PSWD Card

These PSWD cards can be issued to the survey participants by lot. The survey data raised later contains no information whatsoever regarding which questionnaire was completed with which PSWD.

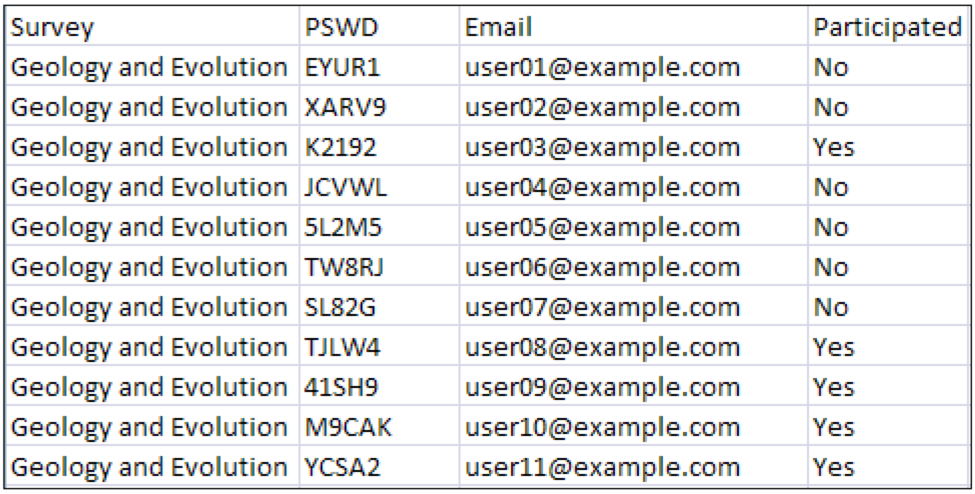
Alternatively, the PSWDs can be sent to the survey participants by batch e-mail. If the recipients' e-mail addresses are known, this procedure can save a great deal of time. With this method it is also guaranteed, that no relationship between the PSWD number and vote can be established.

Participation Tracking

The participation tracking allows the abrogation of participation anonymity whilst still preserving survey anonymity, so as, for example, to verify whether a specific person had actually taken part in an online survey with obligatory participation.

Please note: There is no connection between PSWD and vote here. Therefore, it cannot be ascertained ***how*** a participant has voted.

With this function you can create a CSV file based on a selection of online survey processes specified by the administrator. It contains the name of the survey, the PSWD, the email address to which each PSWD was sent as well as the participation status in the form of a Yes/No indication.

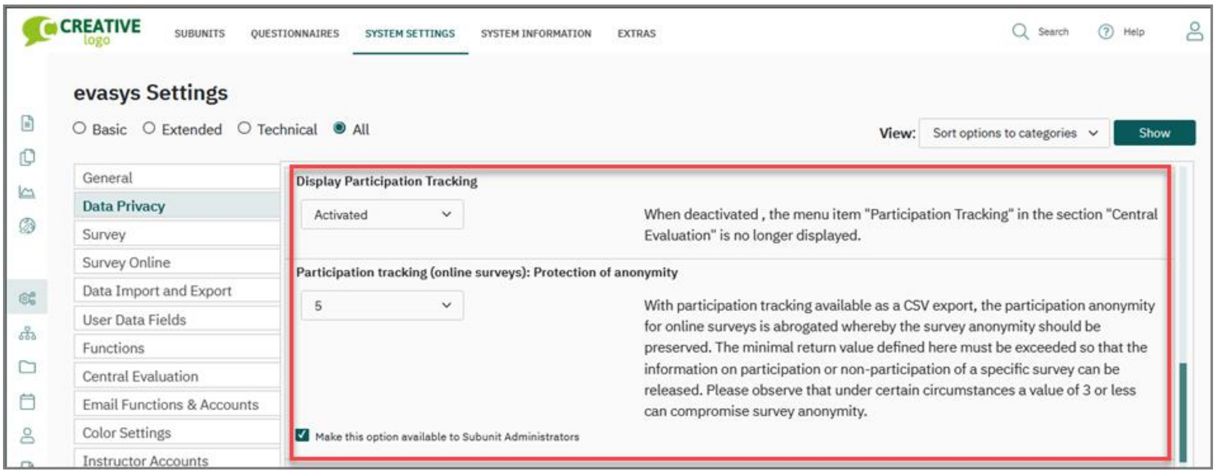


Survey	PSWD	Email	Participated
Geology and Evolution	EYUR1	user01@example.com	No
Geology and Evolution	XARV9	user02@example.com	No
Geology and Evolution	K2192	user03@example.com	Yes
Geology and Evolution	JCVWL	user04@example.com	No
Geology and Evolution	5L2M5	user05@example.com	No
Geology and Evolution	TW8RJ	user06@example.com	No
Geology and Evolution	SL82G	user07@example.com	No
Geology and Evolution	TJLW4	user08@example.com	Yes
Geology and Evolution	41SH9	user09@example.com	Yes
Geology and Evolution	M9CAK	user10@example.com	Yes
Geology and Evolution	YCSA2	user11@example.com	Yes

Figure 3: Example CSV File of Participation Tracking

So as to avoid being able to identify the origin of resulting datasets when returns are very low, the system has a pre-configured minimum return rate of five questionnaires to enable participation tracking to be created for the relevant survey. Optionally, the administrator can increase or decrease this threshold, whereby it is clearly stated that a threshold of 3 or less may compromise survey anonymity.

There is the option of removing the anonymity protection function for participation tracking from the Subunit Administrators.



evasys Settings

○ Basic ○ Extended ○ Technical ● All

View: Sort options to categories Show

Display Participation Tracking

Activated

When deactivated , the menu item "Participation Tracking" in the section "Central Evaluation" is no longer displayed.

Participation tracking (online surveys): Protection of anonymity

5

With participation tracking available as a CSV export, the participation anonymity for online surveys is abrogated whereby the survey anonymity should be preserved. The minimal return value defined here must be exceeded so that the information on participation or non-participation of a specific survey can be released. Please observe that under certain circumstances a value of 3 or less can compromise survey anonymity.

☑ Make this option available to Subunit Administrators

Figure 4: evasys Settings

Response Rate Notification

If online surveys are carried out as time triggered surveys, you can, with the help of “Scheduled Tasks”, send a notification email when, at a defined point in time, the response rate for a survey falls below a certain threshold. This notification can be sent to the instructor of a course and/or other users of the type 'dean', 'instructor' and 'administrator'. The notification only contains information on the current state of the response rate (e.g. 56%). The recipient is not informed about which participants have already taken part in the survey and which have not.

Time Stamp in the Raw Data

The raw data include the exact time of voting in the form of a time stamp. If there is access to the evasys server, then with aid of an access log (IP addresses) and the raw data, it might be possible to determine exactly which IP address belongs to a specific data set. For this reason, the access log file should be deleted regularly, or logging of IP addresses should be disabled in the configuration of the webserver

1.3.3. Hybrid Surveys

A hybrid survey is a combination of paper and online surveys. The participants receive a paper questionnaire as well as a PSWD for access to an online survey and can select which medium they prefer to take part in the survey. There are two ways to distribute PSWDs and questionnaires:

First, participants can receive PSWDs by batch-email. Here, the same conditions apply as for the online surveys described above. In the attachment these emails contain a PDF version of the questionnaire which can be printed and filled in as an alternative to the online survey. Secondly, the paper questionnaires can be distributed to participants. In the header of the questionnaires the PSWD and/or a QR code for the online survey is displayed.

The paper questionnaires contain serial numbers, i.e. each questionnaire set has its own unique number. The serial number of a questionnaire is linked to the corresponding PSWD. Thereby it is guaranteed, that a participant can only produce one dataset (either paperbased or online).

When sending the PSWDs and questionnaires via email, there is no possibility of a correlation between the PSWD and the vote in the survey data. When distributing paper questionnaires, it must be ensured, that they are shared out randomly, as otherwise it may be possible to identify the dataset of a specific participant by means of the serial number.

1.3.4. Non-Anonymous Surveys

Surveys in evasys are conducted by default under the assumption and of course protection of the survey participants’ anonymity. Should the identification of the survey participants be required, for the participant’s address, or later for the evaluation of the survey results, relevant corresponding user data for a course can be imported and utilized. Conducting a non-anonymous survey is possible as a paper based as well as an online survey. As soon as user data is imported for a course, the system assumes that the course is to be evaluated as a non-anonymous survey. It is therefore the responsibility of the user to prevent an abuse of this function.

In a questionnaire of a non-anonymous survey, placeholders for the participant’s identity must be inserted into the header.

Evasys provides reference texts for anonymous and non-anonymous surveys which will be used automatically when sending the PSWDs to your online survey participants.

a) Email: Footnote for anonymous online surveys

> ---
>
> Note: This email has been created automatically. The password indicated in this E-MAIL cannot be traced to you. Your vote is anonymous.

b) Email: Footnote for non-anonymous online surveys

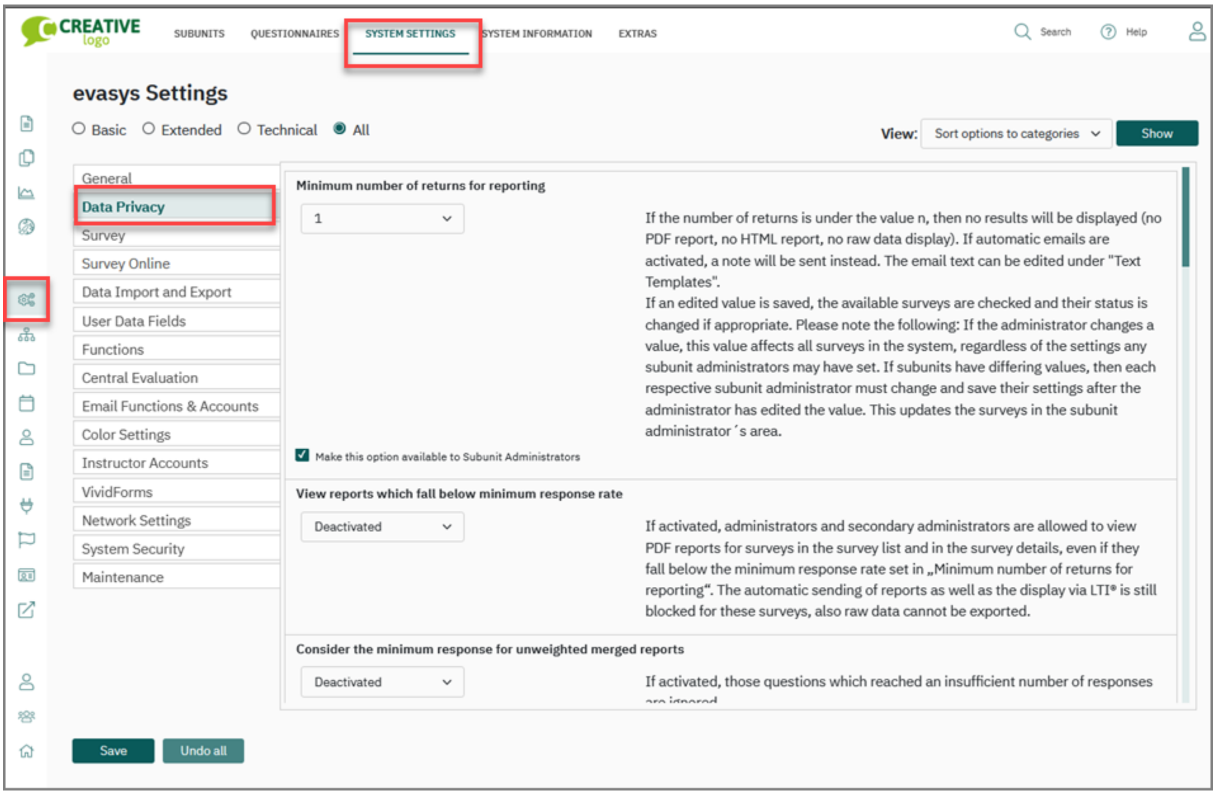
> ---
>
> Note: This survey is non-anonymous. If you take part in this survey with the above named PSWD, your given answers can be associated with you.

The preset content of these text templates can be customized by the administrator.

1.4. Configuration Settings

The most important settings for a data privacy compliant usage of evasys are bundled in “System Settings/evasys Settings” in the submenu “Data Privacy”.

The setting of data privacy options is compliant with the GDPR.



evasys Settings

○ Basic ○ Extended ○ Technical ● All

View: Sort options to categories

Minimum number of returns for reporting

1

If the number of returns is under the value n, then no results will be displayed (no PDF report, no HTML report, no raw data display). If automatic emails are activated, a note will be sent instead. The email text can be edited under "Text Templates".
If an edited value is saved, the available surveys are checked and their status is changed if appropriate. Please note the following: If the administrator changes a value, this value affects all surveys in the system, regardless of the settings any subunit administrators may have set. If subunits have differing values, then each respective subunit administrator must change and save their settings after the administrator has edited the value. This updates the surveys in the subunit administrator´s area.

☑ Make this option available to Subunit Administrators

View reports which fall below minimum response rate

Deactivated

If activated, administrators and secondary administrators are allowed to view PDF reports for surveys in the survey list and in the survey details, even if they fall below the minimum response rate set in „Minimum number of returns for reporting“. The automatic sending of reports as well as the display via LTI® is still blocked for these surveys, also raw data cannot be exported.

Consider the minimum response for unweighted merged reports

Deactivated

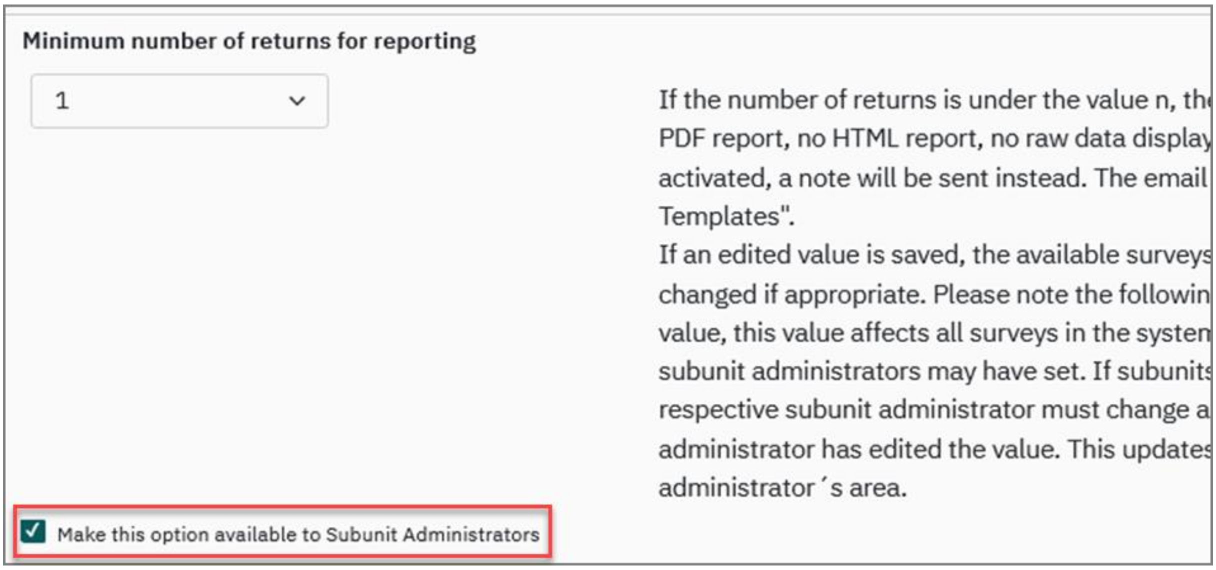
If activated, those questions which reached an insufficient number of responses are ignored

Figure 5: evasys Data Privacy Settings

The evasys Administrator can define system-wide settings in this menu. For some options, Subunit Administrators may be allowed to choose other settings for their areas than the system-wide settings. To grant this, the checkbox “Make this option available to Subunit Administrators” has to be set by the Administrator.

If required, these system settings can be locked by evasys GmbH. When a system setting is locked, there is no possibility for the customer to change this setting, not even for the evasys administrator.

If subsequent changes are necessary, a written notification is requested. In this case, evasys GmbH will unlock the system until the changes have been made.



Minimum number of returns for reporting

1

If the number of returns is under the value n, th
PDF report, no HTML report, no raw data display
activated, a note will be sent instead. The email
Templates".
If an edited value is saved, the available surveys
changed if appropriate. Please note the followin
value, this value affects all surveys in the systen
subunit administrators may have set. If subunits
respective subunit administrator must change a
administrator has edited the value. This updates
administrator´s area.

☑ Make this option available to Subunit Administrators

Figure 6: Make this option available to Subunit Administrators

The following settings are available:

Minimum number of returns for reporting (SUB)

If the number of returns is under the value “n” there will be no display of the results (no PDF report, no HTML report, no raw data). Instead, there will be a note in the letter (the function “generate letter” must be ACTIVATED). The note can be edited at “System Settings/Text Templates”.

Consider the minimum response for unweighted merged reports (SUB)

If activated, those questions which reached an insufficient number of responses are ignored. This function refers to the values for relative and absolute responses defined for the corresponding PDF report. When deactivated, every question will be included into the unweighted merged report.

Anonymization threshold (SUB)

The given value defines the number of returns (questionnaires) up to which the text of open questions has to be anonymized before being displayed. If the number of returns exceeds this value, the scanned images of the open questions are used.

If an edited value is saved, the available surveys are checked, and their status is changed if appropriate. Please note the following: If the administrator changes a value, this value affects all surveys in the system, regardless of the settings any subunit administrators may have set. If subunits have differing values, then each respective subunit administrator must change and save their settings after the administrator has edited the value. This will update the surveys in the subunit administrator´s area.

Display Participation Tracking

When deactivated, the menu item "Participation Tracking" in the section "Central Evaluation" is no longer displayed. To protect anonymity, the minimum response rate for displaying participation tracking can be defined in the system settings, option "Participation tracking (online surveys): Protection of anonymity".

Participation tracking (online surveys): Protection of anonymity (SUB)

With participation tracking available as a CSV export, the participation anonymity for online surveys is abrogated whereby the survey anonymity should be preserved. The minimal return value defined here must be attained so that the information on participation or non-participation of a specific survey can be released. Please observe that under certain circumstances a low value can compromise survey anonymity.

Delete answers to open questions (SUB)

Activates/Deactivates the possibility as an administrator to delete single answers to open questions. This function can be used to delete inappropriate answers and can be accessed in the survey list for each survey.

Permit data export for open questions

When activated, the CSV raw data files also receive the responses to open questions collected in online surveys or after anonymization. For non-anonymized images the "Placeholder image files" will be used (see below).

Anonymous saving of deleted surveys

Deleted surveys are kept anonymously in a wastebasket so that the report creator can generate an accumulated subunit report.

Subunit administrator: View the original recognized forms

If this option is activated, then subunit administrators can view recognized forms as PDF files. If this option is deactivated and if also the following option "View Survey Results" is deactivated, subunit administrators can be completely excluded from accessing survey results.

Subunit administrator: View survey results

If this function is deactivated, then subunit administrators have no authorization to view or export survey results. If this option is deactivated and if also the preceding option "View the original recognized forms" is deactivated, subunit administrators can be completely excluded from accessing survey results.

2. Data Access Rights in evasys

With regard to data access rights, evasys can be configured freely. The following listed functions show the pre-defined settings as far as access rights relating to personal data are concerned.

A tick ✓ symbolizes the availability of the named function. Ticks (✓) in parenthesis show functions which can be switched on and by the administrator.

Description	
Administrator can generate surveys	✓
Administrator can administrate courses/topics	✓
Administrator can view centrally generated survey results	✓
Administrator can view activated instructor/trainer/project accounts and their surveys and results	✓
Administrator can archive raw data from surveys	✓
Administrator can issue viewing rights to quality overviews	✓
Administrator can set notification for noticeable results of quality management	✓
Administrator can delete answers to open questions	✓
Administrator can categorize answers to open questions	✓
Subunit Administrator can generate surveys	✓
Subunit Administrator can administrate courses/topics	✓
Subunit Administrator can view centrally generated survey results from one or more specific subunits.	(✓)
Subunit Administrator can view active instructor/trainer/project accounts and their surveys and results	(✓)
Subunit Administrator can archive raw data from surveys	(✓)
Subunit Administrator can issue viewing rights to quality overviews	(✓)
Subunit Administrator can set notification for noticeable results of quality management	(✓)
Subunit Administrator can delete answers to open questions	✓
Subunit Administrator can categorize answers to open questions	✓
Data Entry Assistant can see complete scanned forms	(✓)
Verifier can see complete scanned forms	(✓)

Table 1: Configuring Data Access Rights, Part 1

Description	
Report Creator can create compressed reports for the President/reports of the overall indicators	(✓)
Report Creator can create compressed reports for Deans/Managers/reports of the indicators	(✓)
Report Creator can create compressed reports for Deans of Studies/Program Managers	(✓)
Report Creator can compare profile lines from reports and surveys (central evaluation)	✓
Report Creator can compare profile lines from reports and surveys (activated accounts)	(✓)
Report Creator can create anonymized subunit reports	✓
Report Creator can create anonymized program of study/group reports	(✓)
Report Creator can create instructor/trainer/project profiles	(✓)
Users of an active instructor/trainer/project account can see their own system folder (centrally generated surveys)	(✓)
Dean/Manager/ Department Head can receive automatic copies of evaluations via e-mail	(✓)*

Table 2: Configuring Data Access Rights, Part 2

* These copies can also be created without open questions

In the following table the data access rights of the administrator and subunit administrator will be compared:

Subunits	Administrator	Subunit Administrator
Access Subunits	Full Access	Own Subunit(s)
Add, Delete Subunits	Full Access	Not allowed
Edit Subunits	Full Access	Own Subunit(s)
Create, Edit, Delete Users	Full Access	Own Subunit(s)
Reports	Full Access	Own Subunit(s)
Archiving	Full Access	Own Subunit(s)
Tree Structure	Full Access	Own Subunit(s)
Generate Surveys	Full Access	Own Subunit(s)
Display Surveys	Full Access	Own Subunit(s)
Delete Surveys	Full Access	Own Subunit(s)
Instructor’s Optional Questions	Full Access	Own Subunit(s)
Batch Events	Full Access	Own Subunit(s)
Display Courses	Full Access	Own Subunit(s)
Scheduled Tasks	Full Access	Own Subunit(s)

Table 3: Data Access Rights of the Administrator and Subunit Administrator, Part 1

Subunits	Administrator	Subunit Administrator
Data Import	Full Access	Own Subunit(s)
Batch Export	Full Access	Own Subunit(s)
Participation Tracking	Full Access	Own Subunit(s)
Access QM-Views	Full Access	Depends on settings of the administrator: - No QM views - Only own subunit(s) - Unrestricted access
QM-Report Dispatch	Full Access	Own Subunit(s)
QM Notification	Full Access	Own Subunit(s)
Current Users Overview	Full Access	Full Access
Questionnaires	**Administrator**	**Subunit Administrator**
Questionnaires	Full Access	Own Questionnaires only; questionnaires of the administrator can be copied, if access is allowed by the administrator.
VividForms Editor	Full Access	Full Access, if Question library access is set.
VividForms Designer	Full Access (if licensed)	Depends on settings of the administrator
Question Library	Full Access	If granted: Full Access (own questions) Read Only Access (questions of the administrator and public questions).
System Settings	**Administrator**	**Subunit Administrator**
Text Templates	Full Access	Own Questionnaires only (in the details of a questionnaire)
Documents	Full Access	Use existing, add own
Report Settings	Full Access	Own Subunit(s)
Online Templates	Full Access	Limited Access; depends on settings of the administrator: - Defined by Administrator (No access) - Templates only - Unrestricted access

Table 4: Data Access Rights of the Administrator and Subunit Administrator, Part 2

System Settings	Administrator	Subunit Administrator
evasys Settings	Full Access	Own Subunit(s) Depends on settings of the administrator (“Make this option available to subunit administrators”); system-wide settings can only be defined by the administrator
Panel Management	Full Access	Own Subunit(s)
Define Tree Structure	Full Access	Not accessible
Course Types	Full Access	Not accessible
Periods	Full Access	Not accessible
Custom Titles	Full Access	Not accessible
Process Defaults	Full Access	Limited Access
Web Service Settings	Full Access	Not accessible
Language Sets	Full Access	Not accessible
Own User Profile	Full Access	Full Access
Administrators	Full Access	Not accessible
Organization Profile	Full Access	Not accessible
System Information	Administrator	Subunit Administrator
Search Function	Full Access	Own Subunit(s)
Send E-Mail	Full Access	Full Access
Utilization Statistics	Full Access	Own Subunit(s)
System Summary	Full Access	Own Subunit(s)
License	Full Access	Not accessible
Send Email to Support	Full Access	Full Access
System Cleaning	Full Access	Not accessible
System Status	Full Access	Full Access
Manuals	Full Access	Full Access
Sample Files	Full Access	Full Access
Deliveries	Full Access	Own Subunit(s)
Log Book	Full Access	Own Subunit(s) and General Logs
Deletion Log	Full Access	Full Access
Web Service Log	Full Access	Full Access
Mail Service Log	Full Access	Full Access

Table 5: Data Access Rights of the Administrator and Subunit Administrator, Part 3

3. Data Privacy Protection

3.1. Definitions

Evasys is an automated system on which personal data is processed according to Article 4 General Data Protection Regulation (GDPR).

For the purposes of this Regulation:

(1)

‘personal data’ means 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;

(2)

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3.2. Controller

Controller for the personal data of an evasys system is always the organization which uses evasys to collect the data and therefore not evasys GmbH. This applies accordingly to evasys systems which are hosted by evasys GmbH.

3.3. Delivery of Evaluations

Evasys sends emails with evaluations of surveys to the evaluated parties and also offers the ability to inform managing bodies (i.e. Deans) on the results of single surveys. The Acrobat PDF has proved to be the electronic document format of choice.

The delivery of results via email requires a consent under Article 7 GDPR. This consent is usually given by an operating agreement or evaluation order outside of evasys.

It is possible to set a password in “System Settings/evasys Settings/Email Functions & Accounts” to encrypt the sent PDF-reports. If a password is defined in “Password protection for reports sent by email”, reports that are sent by email require the password to open. If no password is defined, no password is required. The password is a general, system-wide password.

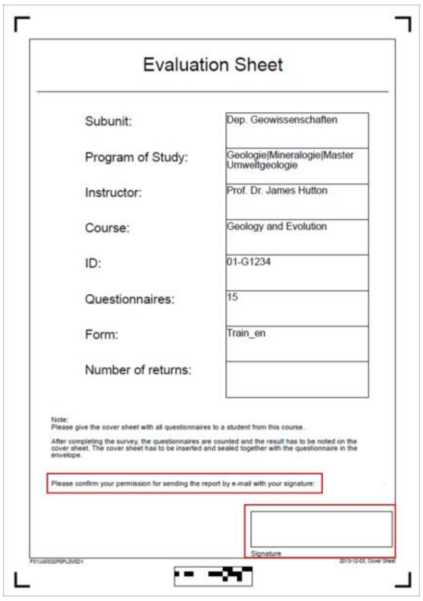
Note:

- The password protection does not work for PDF/A reports. These reports are not protected.
- This setting does not affect the mailing functions of user accounts.
- Password protected reports cannot be edited with PDF editors.

- Depending on the compatibility of the plug-in, PDF report plug-ins might not work with passwords.

The password cannot exceed 32 characters. Allowed characters: a-Z, 0-9, ,;.:-_?!"$%&/()+*~#´|<>. Blank characters are not allowed.

When using the cover sheet method, the evaluated person can declare his/her consent on a signature field on the cover page. If the signature is missing, automatic sending of results is suppressed for this person.



Evaluation Sheet

Subunit:	Dep. Geowissenschaften
Program of Study:	Geologie|Mineralogie|Master Umweltgeologie
Instructor:	Prof. Dr. James Hutton
Course:	Geology and Evolution
ID:	01-G1234
Questionnaires:	15
Form:	Train_en
Number of returns:	

Note:
Please give the cover sheet with all questionnaires to a student from this course.

After completing the survey, the questionnaires are counted and the result has to be noted on the cover sheet. The cover sheet has to be inserted and sealed together with the questionnaire in the envelope.

Please confirm your permission for sending the report by e-mail with your signature:

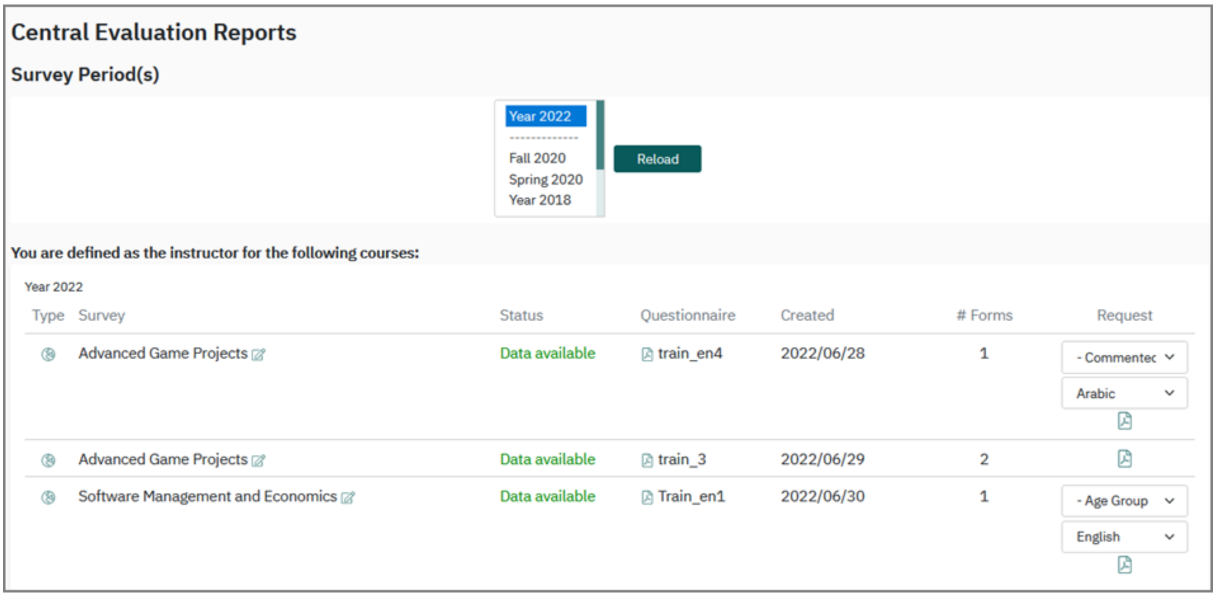
Signature

P51U45532P0PL0V0D1

2013-12-03, Cover Sheet

Figure 7: Cover Sheet with signature field

As an alternative to sending the reports by email, the results can be accessed by using the so-called “Pull Method” directly by the evaluated person from the evasys server. Here, an SSL encryption is used.



Central Evaluation Reports

Survey Period(s)

Year 2022

Fall 2020
Spring 2020
Year 2018

You are defined as the instructor for the following courses:

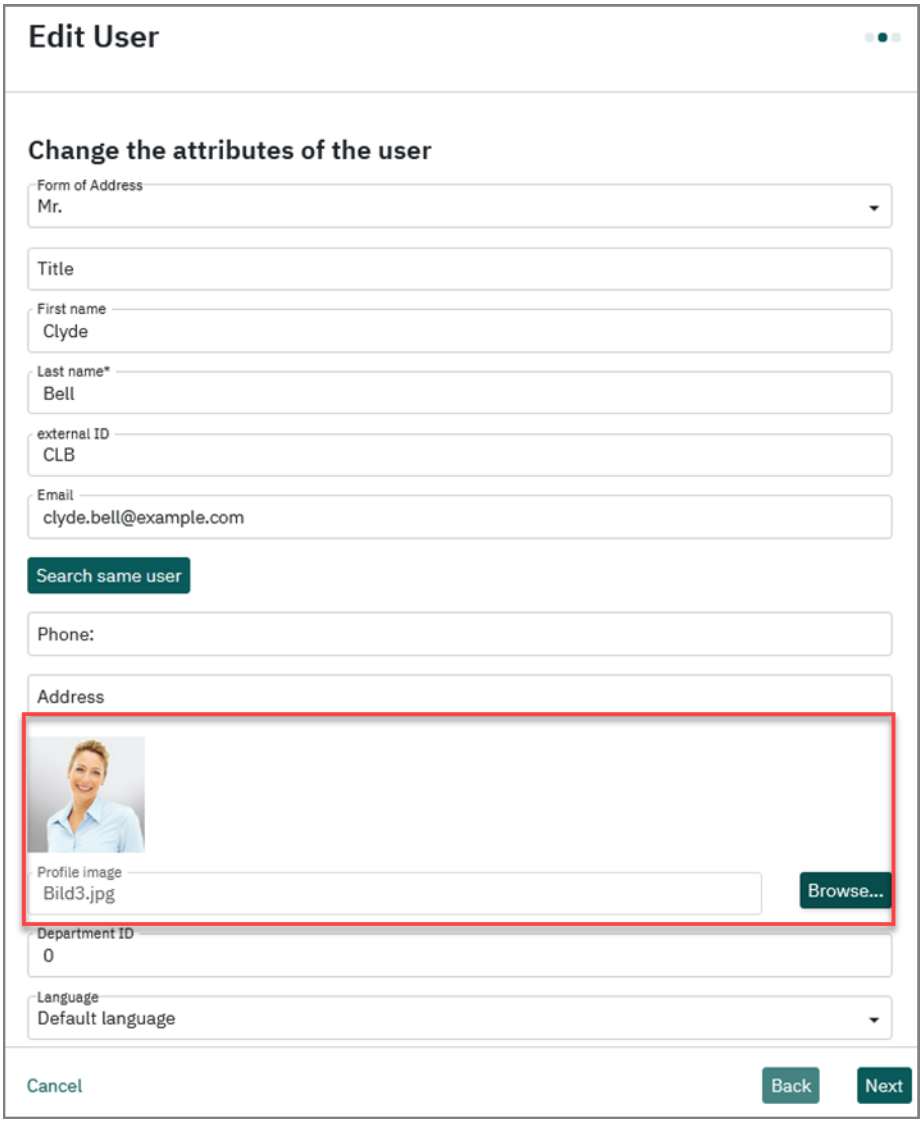
Year 2022

Type	Survey	Status	Questionnaire	Created	# Forms	Request
	Advanced Game Projects	Data available	train_en4	2022/06/28	1	- Commentec Arabic
	Advanced Game Projects	Data available	train_3	2022/06/29	2	
	Software Management and Economics	Data available	Train_en1	2022/06/30	1	- Age Group English

Figure 8: Pulling reports

3.4. Profile Images

A profile image can be uploaded in the user profile of an instructor (trainer / project manager). This profile image can be displayed in the survey header of online surveys, on PSWD cards or in the list of surveys shown to participants after they have taken part in an online survey. If an instructor's portrait is chosen as a profile image you have to ensure that the instructor has been asked for permission.



Edit User

Change the attributes of the user

Form of Address: Mr.

Title

First name: Clyde

Last name*: Bell

external ID: CLB

Email: clyde.bell@example.com

Phone:

Address

Profile image: Bild3.jpg

Department ID: 0

Language: Default language

Figure 9: Profile Image

3.5. Technical and Organizational Measures

Article 8 GDPR, (1): Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

In the following sections, the various technical and organizational measures provided by evasys are listed.

3.5.1. Access Control

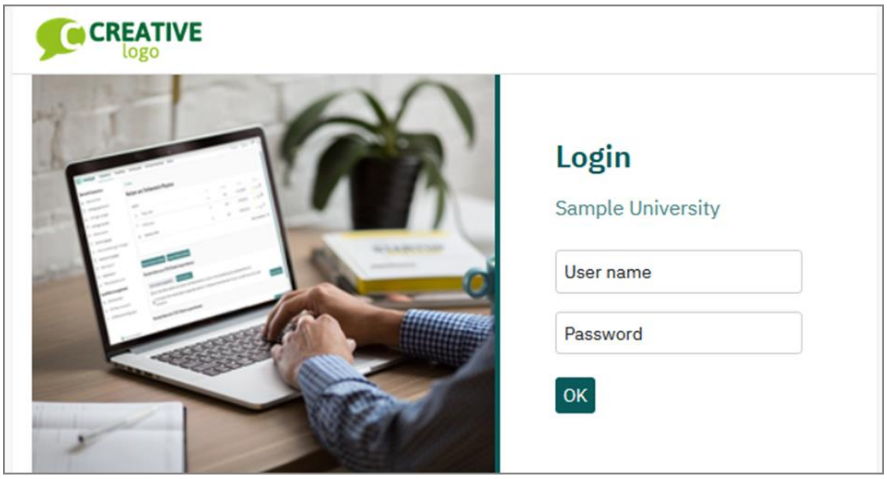


Figure 10: evasys Log In Screen

a) Web server: Access to the evasys system is only possible for persons with authorization in the form of a user name and password.
   A policy for using secure passwords can be activated. See chapter B.2. Measures to Seal off the Server.
b) Access to the evasys system PC is only possible for authorized persons (users at the operating system level) with a user name and password.

3.5.2. Data Media Control

The data media of the operating system on which evas

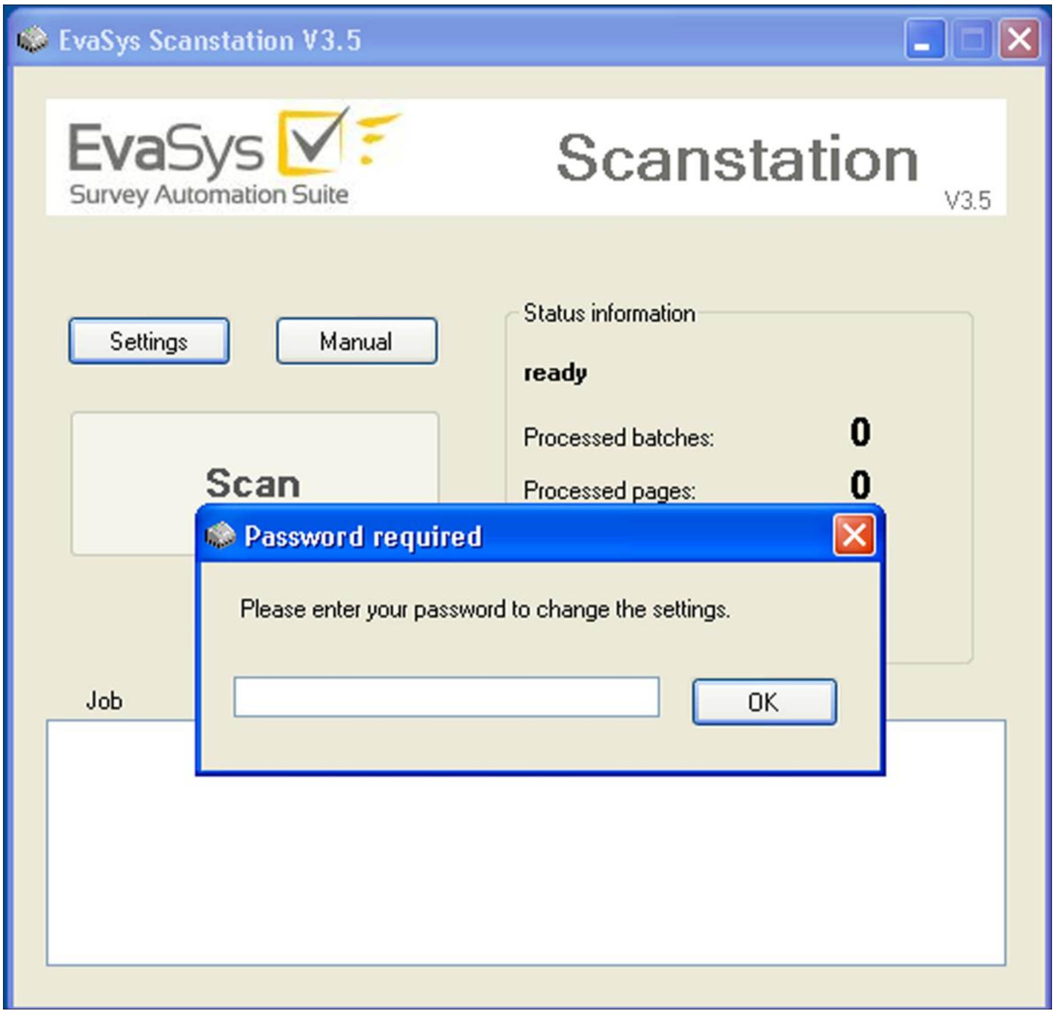
ys is installed, cannot be addressed over the network and may only be accessed locally by authorized personnel.

The personal data in evasys is stored in the used database (MySQL or MS SQL). In the default installation, communication with the database takes place exclusively via the local web server. In addition, technicians from evasys can, in accordance, access the database indirectly for maintenance purposes, provided that the organization responsible allows and enables this.

3.5.3. Storage Control

Access to raised data is restricted to administrators and users of active instructor/trainer accounts or project accounts to their own surveys. The generation of survey data takes place

- In paper-based surveys: via the scan station, operated by trained or authorized personnel. Access to the scan station should be restricted accordingly. For this reason, the configuration dialogue of the scan station software is protected by a password.



EvaSys Scanstation V3.5

Status information

ready

Processed batches: 0

Processed pages: 0

Password required

Please enter your password to change the settings.

Figure 11: evasys Scan Station

- In online surveys: Participants of online surveys can complete the questionnaire once, the authorization number (PSWD) expires after use.

Using the deletion protocol, all important deletions ever made in evasys can be reconstructed. It is not possible to delete entries from this protocol.

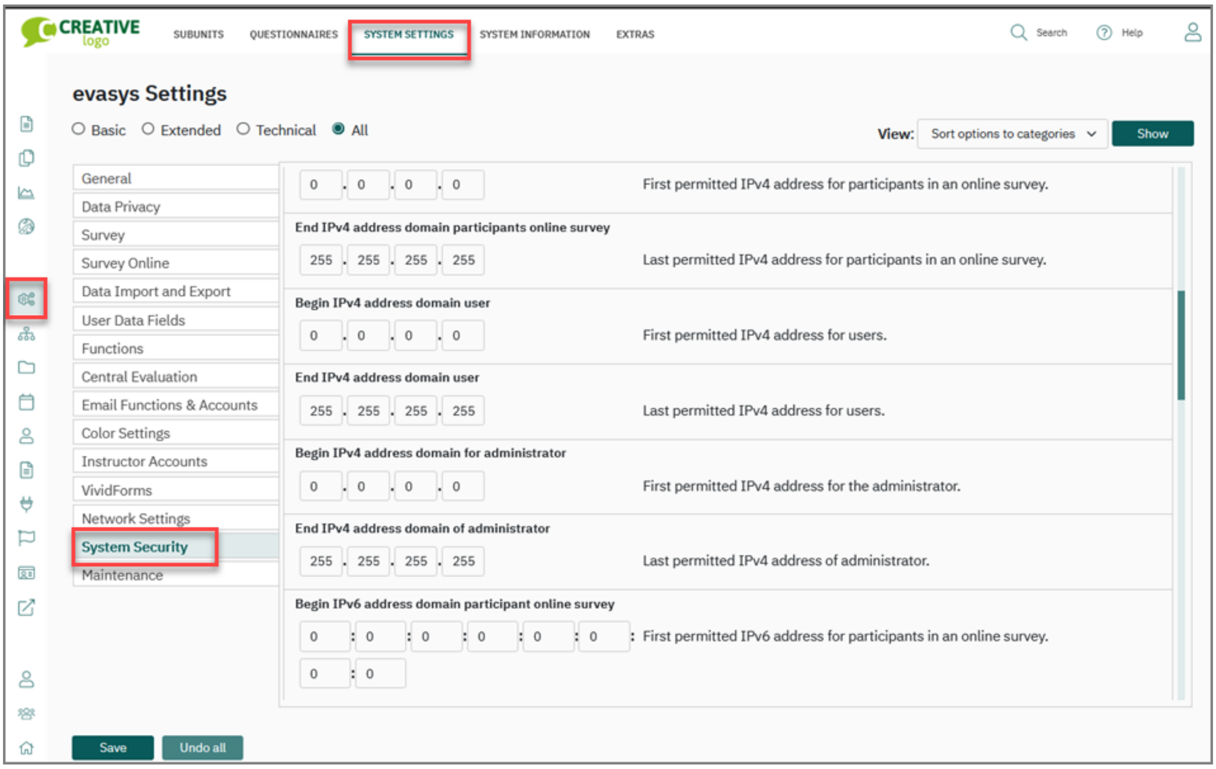
The following deletion processes are recorded:

- Subunits
- Users
- Study Courses
- Surveys
- PSWD's
- Questionnaires
- Folders (of active instructors/trainers/projects)

To each deletion process, the following information is recorded:

- User: Who deleted?
- Type of Object and description: What was deleted?
- Date: When was it deleted?
- ID of the trigger process: Through which other deletion process was this deletion triggered?

3.5.4. User Control



0 . 0 . 0 . 0 — First permitted IPv4 address for participants in an online survey.

End IPv4 address domain participants online survey: 255 . 255 . 255 . 255 — Last permitted IPv4 address for participants in an online survey.

Begin IPv4 address domain user: 0 . 0 . 0 . 0 — First permitted IPv4 address for users.

End IPv4 address domain user: 255 . 255 . 255 . 255 — Last permitted IPv4 address for users.

Begin IPv4 address domain for administrator: 0 . 0 . 0 . 0 — First permitted IPv4 address for the administrator.

End IPv4 address domain of administrator: 255 . 255 . 255 . 255 — Last permitted IPv4 address of administrator.

Begin IPv6 address domain participant online survey: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 — First permitted IPv6 address for participants in an online survey.

Figure 12: Determining the Authorized IP Address Ranges

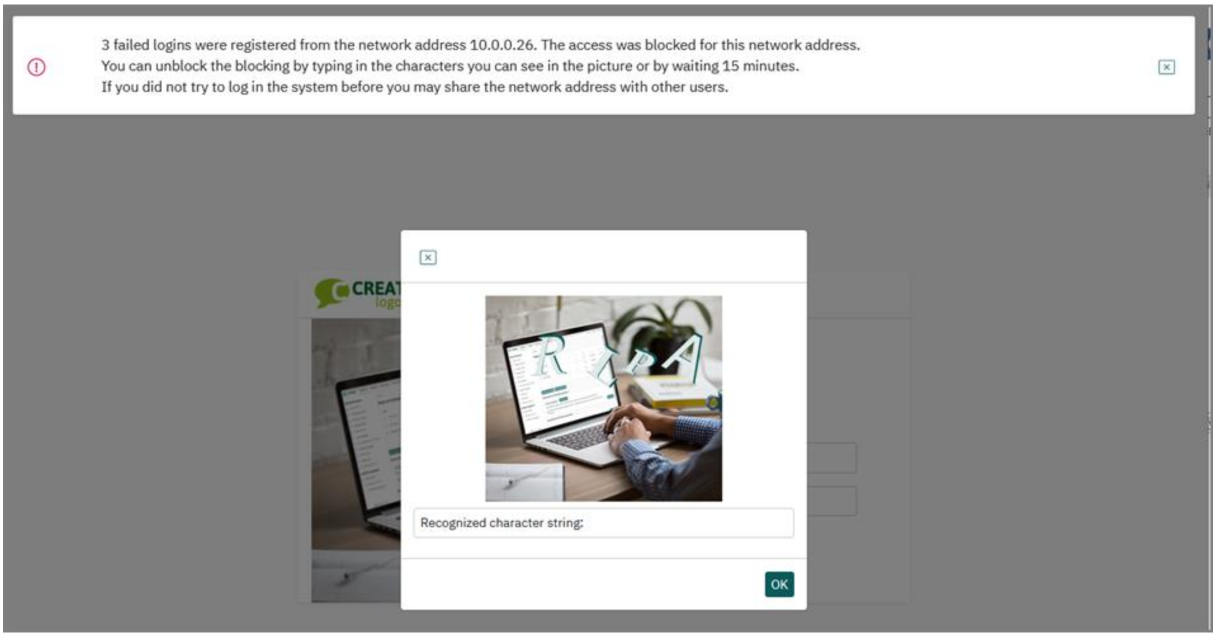
- The browser access, depending on the user level, is restricted to specific IP address ranges.

In this way,

- Participants of online surveys
- Operators of user accounts
- Administrator and subunit administrators

may only gain access from specific IP addresses, which can be separately predefined for each of these user roles.

- Access is only enabled after authorization via user name and password.
- The communication between the evasys web server and the browser program of the user is cryptographically encoded (128 bit SSL) and therefore tap-proof.
- Through access control measures on the part of the computer center of the organization responsible, an important contribution to the security of the evasys system is made.
- Evasys offers you the possibility of blending in a so-called CAPTCHA graphic, after a defined number of failed logins (default: 3) from an IP address. This function protects evasys from automated attacks. CAPTCHAs are graphics in which figures (numbers or alphabetical characters) are displayed, so that machines cannot read them. They are employed to detect whether the counterpart is a human being or a machine. If CAPTCHAs are activated, after multiple failed login attempts the user is prompted to enter a CAPTCHA:



3 failed logins were registered from the network address 10.0.0.26. The access was blocked for this network address.
You can unblock the blocking by typing in the characters you can see in the picture or by waiting 15 minutes.
If you did not try to log in the system before you may share the network address with other users.

Figure 13: CAPTCHA Function After Several Failed Logins

3.5.5. Access Control

Depending on user type, only specific information can be recalled:

Active Instructor/Trainer/Project Account

Users can only access their own surveys and the results therein. The user can also access the survey results affecting him from the Central Evaluation, provided the Administrator allows this.

Passive Instructor/Trainer/Project Account

If the instructor/trainer/project account is switched to passive, then the user can only view the survey results affecting him from the Central Evaluation, provided the Administrator allows this.

Data Entry Assistant

The user designated to anonymize written comments can access the written comments in order to anonymize and categorize them. As part of this anonymization, the Data Entry Assistant can view the complete scanned questionnaire page of a question that is to be made anonymous.

The administrator can deactivate the data entry assistant's option to view the complete scanned questionnaire page.

The administrator can limit access by the data entry assistant to one or more Subunits.

Report Creator

This user type can request anonymized subunit reports (central and decentral evaluation) as well as program of study/group reports and instructor/trainer/ project reports (central evaluation).

The report creator can be granted access to one subunit, several subunits or all subunits (system-wide).

Subunit Administrator

The subunit manager has full access to all centrally raised data from one or more subunits.

The administrator can deactivate the subunit administrator’s right to view survey results. The administrator can also deactivate the subunit administrator’s option to view scanned questionnaires.

The administrator can assign the subunit administrator the additional roles of report creator, verifier and data entry assistant. This can all be done in one profile.

Administrator

The administrator has full access to all centrally raised data. The administrator can also activate and realize the roles of report creator, verifier and data entry assistant directly in his/her own profile.

Dean of Studies or Program Manager (only central evaluation)

The operator of this user profile can make a selection from a list of evaluated courses/topics, which are then individually summarized by the report creator in a report.

Dean or Manager or Department Head

The operator has access to a complete application statistic for their own subunit.

This user account can be switched passive or active. An active dean or department head can view his own surveys and, for example, access the enabled QM screens (Phase 5). A passive account has access solely to the individually released QM screens and to the survey results affecting him from the central evaluation, provided the administrator allows this.

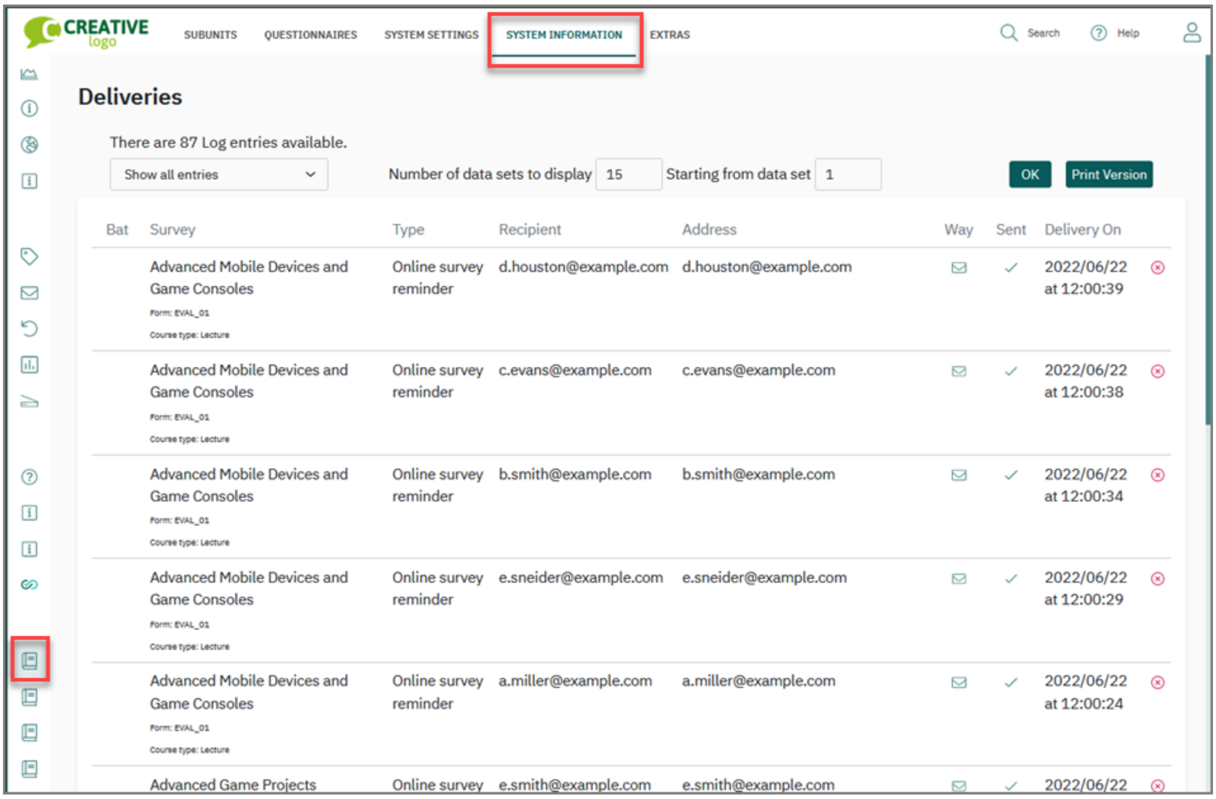
Verifier

The verifier has access to all the surveys which have been released for visual inspection. The administrator can restrict this access to one or several subunits.

During verification the verifier has access to the complete scanned questionnaire containing a question which requires verification. The administrator can deactivate the verifier’s option to view the complete scanned questionnaire page.

3.5.6. Communication Control

The automatic or manual delivery via email of evaluations of surveys is logged by evasys in the delivery table.



Deliveries

There are 87 Log entries available.

Number of data sets to display 15 Starting from data set 1

Bat	Survey	Type	Recipient	Address	Way	Sent	Delivery On
	Advanced Mobile Devices and Game Consoles Form: EVAL_01 Course type: Lecture	Online survey reminder	d.houston@example.com	d.houston@example.com	✉	✓	2022/06/22 at 12:00:39
	Advanced Mobile Devices and Game Consoles Form: EVAL_01 Course type: Lecture	Online survey reminder	c.evans@example.com	c.evans@example.com	✉	✓	2022/06/22 at 12:00:38
	Advanced Mobile Devices and Game Consoles Form: EVAL_01 Course type: Lecture	Online survey reminder	b.smith@example.com	b.smith@example.com	✉	✓	2022/06/22 at 12:00:34
	Advanced Mobile Devices and Game Consoles Form: EVAL_01 Course type: Lecture	Online survey reminder	e.sneider@example.com	e.sneider@example.com	✉	✓	2022/06/22 at 12:00:29
	Advanced Mobile Devices and Game Consoles Form: EVAL_01 Course type: Lecture	Online survey reminder	a.miller@example.com	a.miller@example.com	✉	✓	2022/06/22 at 12:00:24
	Advanced Game Projects	Online survey	e.smith@example.com	e.smith@example.com	✉	✓	2022/06/22

Figure 14: Protocol of Deliveries

Thereby, the time of dispatch is recorded. In addition to this protocol, other relevant protocols of the mail server can be utilized.

The delivery protocol can be deleted using the system cleaning function.

3.5.7. Input Control

The provision of user accounts lies solely with the administrator, or subunit administrator for specific subunits. The time of issue for subunits, instructor accounts and/or interviewer accounts and surveys as well as the return data, is recorded in the database. The return data of scan stations can be related to a workstation using identifying information, so that even when using several scan stations, it can be ascertained, which station transmitted which data at what time.

Every access to user accounts is logged by recording the time stamp and IP address. In this way it can be determined, from which PC the last access was made.

The system protocol of the IIS web server records all access to the system. This access is saved as follows:

IIS:

```
2011-02-12 12:23:15 179.233.122.42 GET /evasys/umfragen.php?stuid=984&mode=show&PHPSESSID=533[…]49728 80
...
```

In this example, the content of the folder #984 of the active instructor account was recalled by the IP address 179.233.122.42. If necessary, it would be possible for a technician from evasys GmbH using a remote maintenance connection, to identify the user account.

3.5.8. Availability control

The evasys documentation describes the relevant folders and procedures for undertaking a failure-free system back-up (see chapter 0 – Additional Relevant Data Protection Information).

3.5.9. Order Control

This is the responsibility of the evasys administrator.

3.5.10. Transport Control

The communication channel between the system (web server) and the operator (browser) encrypted with 128 bit SSL encryption and cannot be tapped or manipulated.

If evasys scan stations are implemented in the generation of survey data, encryption of the transmitted scan data via SSL is also available.

Due to the disproportionate cost of a cryptographic solution[1], the dispatch of evaluation documents via e-mail is unencrypted. The system offers the possibility that the

[1] In order to guarantee that only the correct recipient can decrypt a message, it is necessary to employ a procedure consisting of public as well as private keys. Each potential recipient, using a password and random factors, must generate a key for himself as well as send the simultaneously generated public key to the decryption center. The public key is necessary so that the encryption center can encode the data in such a way, that only the owner of the private key is able to decrypt it again. In order to use this system, the corresponding software (i.e. PGP – Pretty Good Privacy) must be installed on all recipients' PC's. The administration of all these public keys, the large scale installation of the necessary software as well as the data maintenance would mean a disproportionately high administrative expenditure for the organization administration as well as for the users.

unencrypted dispatch be signed for by the recipient, as well as offering transport by regular post.

Another possibility is to make the encrypted results available to those affected (passive instructors/trainers/project managers) at individual request (Pull SSL).

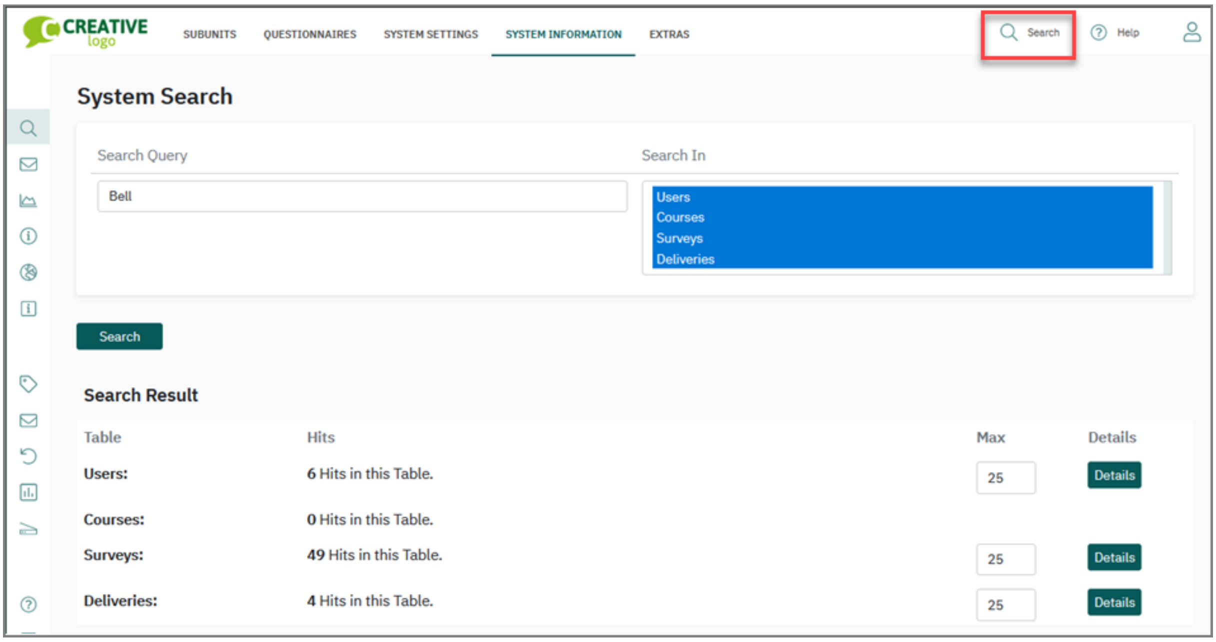
3.5.11. Organization Control

In preparation of the installation of evasys systems, evasys GmbH makes contact with the computer centers of the relevant organization, so as to discuss access restrictions and other aspects of data protection.

3.6. Information (Article 15 GDPR: Right of access by the data subject)

The administrator can access information regarding the stored data at all times and give information.

For his purpose, a system-wide search is implemented:



System Search

Search Query: Bell

Search In: Users, Courses, Surveys, Deliveries

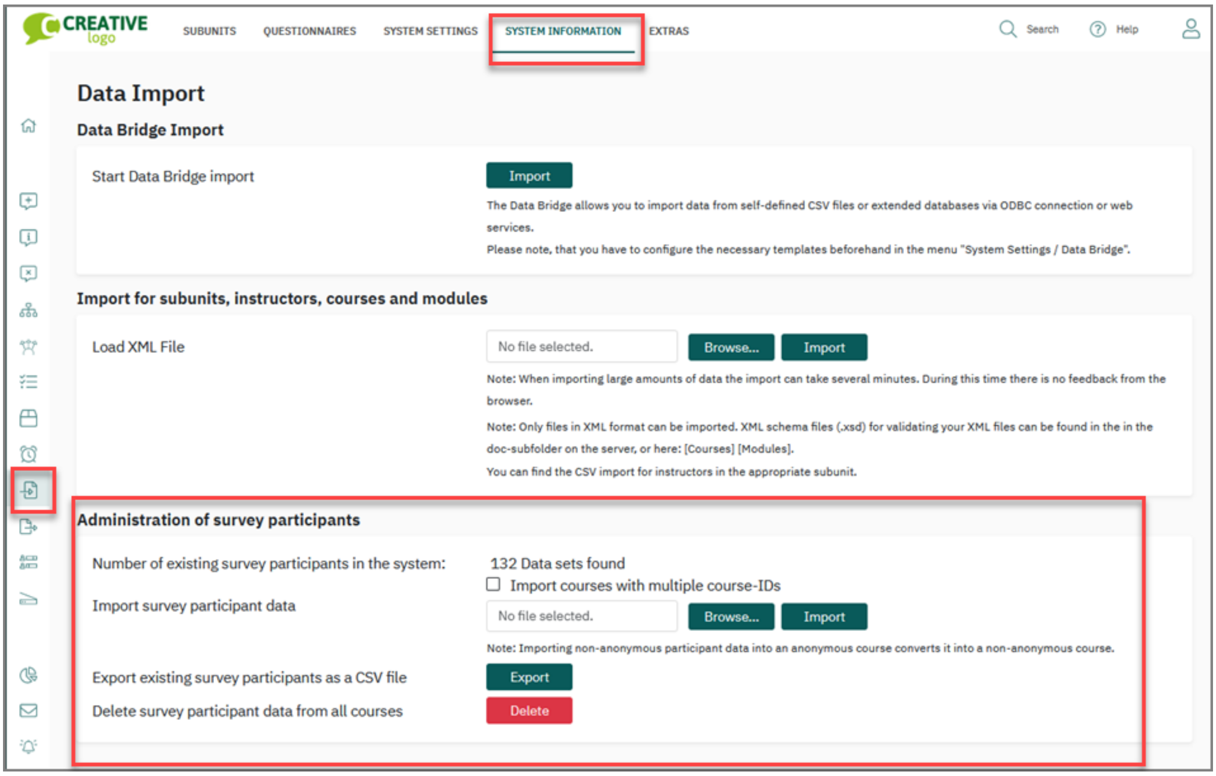
Search

Search Result

Table	Hits	Max	Details
Users:	6 Hits in this Table.	25	Details
Courses:	0 Hits in this Table.		
Surveys:	49 Hits in this Table.	25	Details
Deliveries:	4 Hits in this Table.	25	Details

Figure 15: System search

To search for participant data, the administrator can use the “Administration of survey participants” in “Subunits/Data Import/”:



Data Import

Data Bridge Import

Start Data Bridge import

The Data Bridge allows you to import data from self-defined CSV files or extended databases via ODBC connection or web services.
Please note, that you have to configure the necessary templates beforehand in the menu "System Settings / Data Bridge".

Import for subunits, instructors, courses and modules

Load XML File: No file selected.

Note: When importing large amounts of data the import can take several minutes. During this time there is no feedback from the browser.

Note: Only files in XML format can be imported. XML schema files (.xsd) for validating your XML files can be found in the in the doc-subfolder on the server, or here: [Courses] [Modules].
You can find the CSV import for instructors in the appropriate subunit.

Administration of survey participants

Number of existing survey participants in the system: 132 Data sets found

☐ Import courses with multiple course-IDs

Import survey participant data: No file selected.

Note: Importing non-anonymous participant data into an anonymous course converts it into a non-anonymous course.

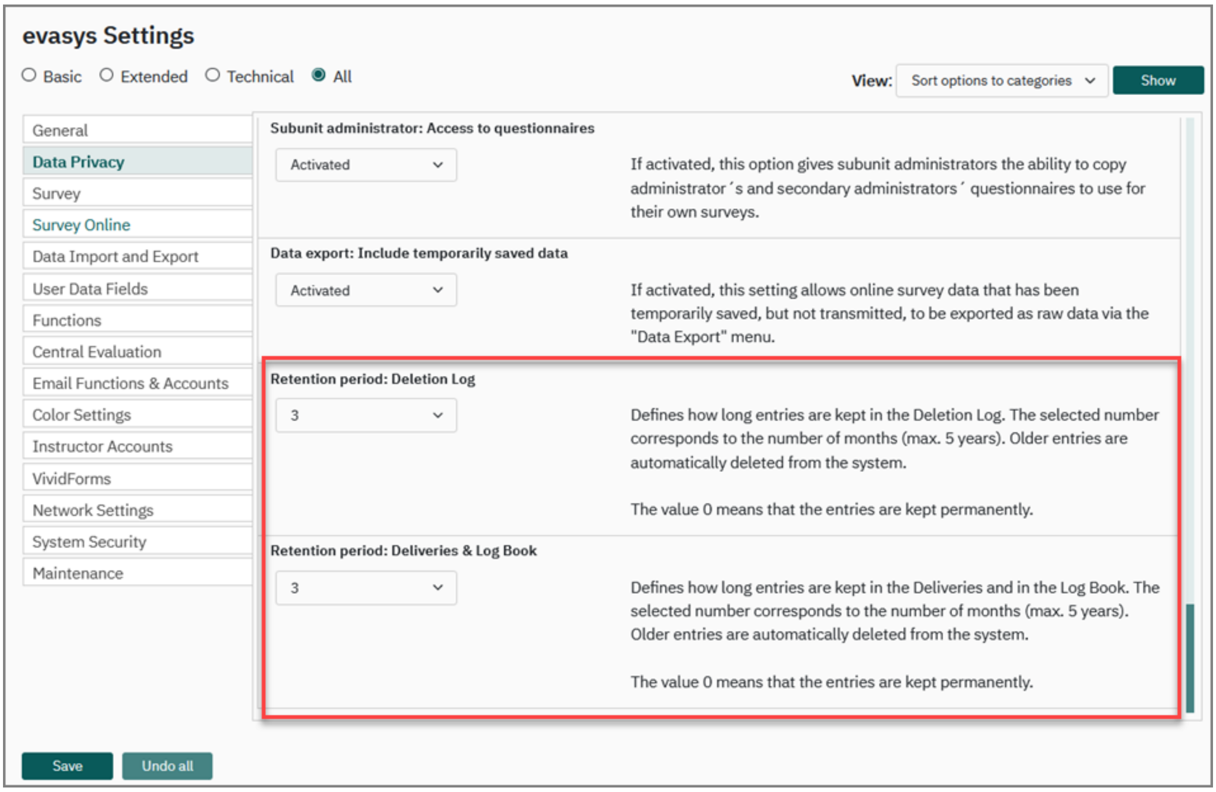
Export existing survey participants as a CSV file

Delete survey participant data from all courses

Figure 16: Participant Administration

3.7. Delete Log Entries

Under "Settings/Configuration" there are two switches to automatically limit the storage duration of log entries. This allows to limit the contents of the deletion log, the delivery logs and the general event log (logbook) to a certain period of time. This prevents personal data contained in the logs from being stored unnecessarily. The period can be extended from 1 month to a maximum of 5 years. Alternatively, the function can be switched off completely.



Subunit administrator: Access to questionnaires

Activated

If activated, this option gives subunit administrators the ability to copy administrator´s and secondary administrators´ questionnaires to use for their own surveys.

Data export: Include temporarily saved data

Activated

If activated, this setting allows online survey data that has been temporarily saved, but not transmitted, to be exported as raw data via the "Data Export" menu.

Retention period: Deletion Log

3

Defines how long entries are kept in the Deletion Log. The selected number corresponds to the number of months (max. 5 years). Older entries are automatically deleted from the system.

The value 0 means that the entries are kept permanently.

Retention period: Deliveries & Log Book

3

Defines how long entries are kept in the Deliveries and in the Log Book. The selected number corresponds to the number of months (max. 5 years). Older entries are automatically deleted from the system.

The value 0 means that the entries are kept permanently.

Figure 17: Retention Period

3.8. Remote Maintenance

For maintenance purposes, the support technicians of evasys may use so called remote maintenance programs, by which travels can be minimized and the fixing of any failures can begin immediately. In accordance with the specifications of the evasys Remote Maintenance (appendix 4.2), this remote maintenance connection can be established via TeamViewer™. The explicit agreement of the organization responsible is a prerequisite.

Any data absorbed during maintenance work are deleted at the end of the service.

If requested, evasys GmbH offers an agreement for remote maintenance access in accordance with Article 15 GDPR.

4. Additional Relevant Data Protection Information

4.1. Backup Specifications

4.1.1. Database

The evasys database contains:

- complete profile data (organization, faculties, users)
- all surveys with raw data as well as statistical characteristics
- the content and evaluation parameters of all questionnaires
- operating data (log books, survey periods, PSWD lists)

You can find information for conducting a backup of the database in the technical manual.

4.1.2. Graphic Files from Open Questions

Answers to open questions are saved as PNG graphic files. These can be found in the folder:

C:\INETPUB\WWWROOT\EVASYS\IMG

Please note, that the actual path can deviate in your system.

Here you will find the images of the open questions as well as the images which are shown in the verifier. The folder structure is defined as [survey period\subunit\user\survey].

To save these files, it is recommended to stop the service and then restart it afterwards.

4.1.3. Scanstation Original Graphic Files

The evasys Scanstation software can create a backup copy from every batch. You can make this backup copy in an archive folder defined in the Scanstation. The exact path to the archive directory can be found in the Scanstation settings, tab “Scan Destination”.

For further information, please consult the Scanstation Manual.

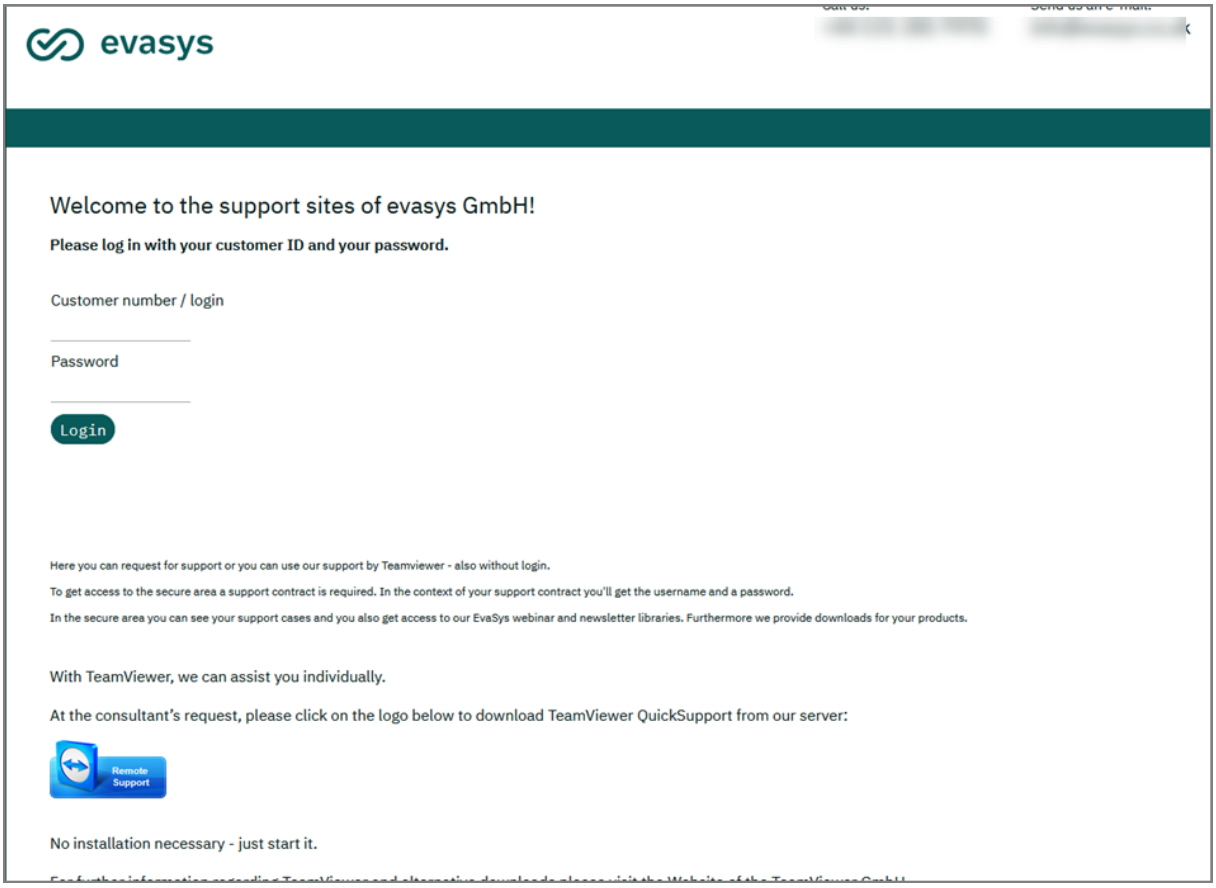
4.2. Remote Maintenance Specifications

In most cases, settling support queries can be solved quickly via telephone or email. However, in complicated cases this method can prove to be protracted and ineffective. In this case, it is recommended that a remote maintenance connection be established.

Remote Maintenance enables the evasys developers to work “virtually” on your evasys server and so to analyze and solve the question at hand. In particular cases, this connection is also used to install updates. It is important to note that such remote maintenance is only possible for a defined period and with your express permission.

For this, evasys GmbH employs the software solution “TeamViewer”. This solution works without any installation of software. You merely start a 300 KB client application by clicking on a link on our web site:

http://support.evasys.de/OnlineSupportSystem



Call us: [redacted] Send us an e-mail: [redacted]

Welcome to the support sites of evasys GmbH!

Please log in with your customer ID and your password.

Customer number / login

Password

Login

Here you can request for support or you can use our support by Teamviewer - also without login.

To get access to the secure area a support contract is required. In the context of your support contract you'll get the username and a password.

In the secure area you can see your support cases and you also get access to our EvaSys webinar and newsletter libraries. Furthermore we provide downloads for your products.

With TeamViewer, we can assist you individually.

At the consultant’s request, please click on the logo below to download TeamViewer QuickSupport from our server:

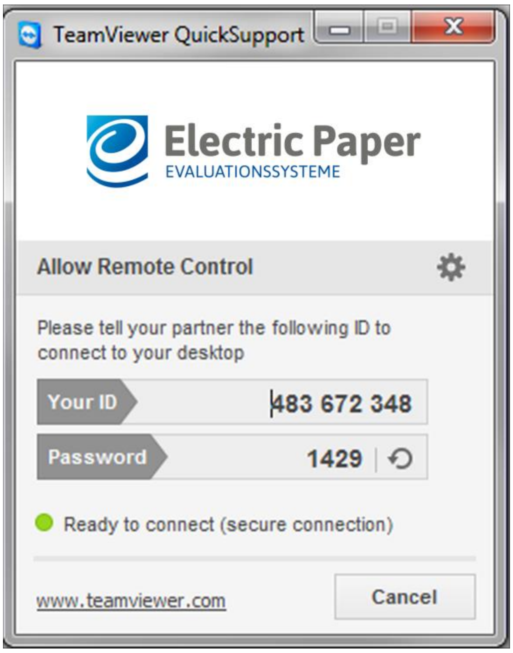
No installation necessary - just start it.

For further information regarding TeamViewer and alternative downloads please visit the Website of the TeamViewer GmbH

Figure 18: File Download

Download the file and save it or execute it directly. Having executed the file, the TeamViewer application opens. In the section “Your ID” a nine-digit ID is displayed, in the section “Password” a four-digit password is displayed.

When asked, tell our supporter the ID and the password so that he can connect to your computer.



TeamViewer QuickSupport

Electric Paper
EVALUATIONSSYSTEME

Allow Remote Control

Please tell your partner the following ID to connect to your desktop

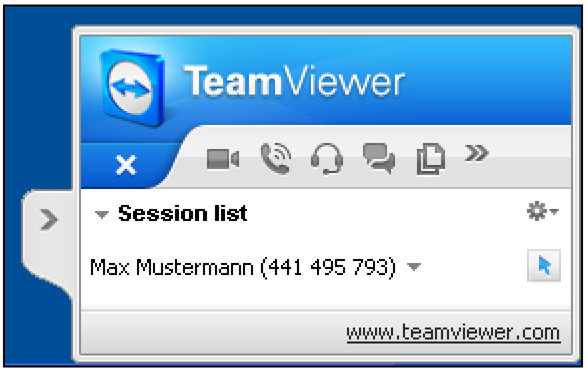
Your ID 483 672 348

Password 1429

● Ready to connect (secure connection)

Figure 19: TeamViewer Interface

As soon as the supporter has connected to your computer, remote control is activated and your screen is transferred. You can see this in the session list which has opened in the lower right corner of the screen.



Max Mustermann (441 495 793)

Figure 20: Activated TeamViewer Session

Now you can observe our support staff working on the system. You can deactivate remote control at any time by clicking the button with the blue arrow next to the name of the supporter. As an alternative, click the arrow next to the name and deactivate the option “Allow control. You can furthermore end the session by clicking the cross-icon or selecting the option “Close connection”.

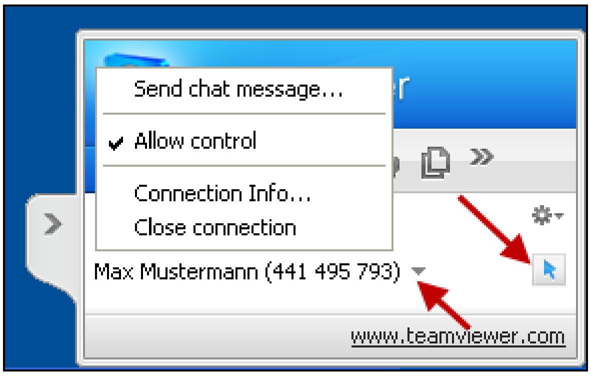


Figure 21: Disable Remote Control

As soon as the maintenance work has been finished, the supporter will close the session.

For further information on security aspects see the TeamViewer website.

4.3. Check for Update Notification

Once the administrator has logged in, automatic checks for updates are carried out at regular intervals (standard value is 30 days). When checking for updates, data is transferred from the evasys system to the update server via the administrator's web browser (the evasys server itself does not connect to the update server). The following information is included:

- the customer name,
- the license key,
- the current evasys version,
- the default system language,
- the current configured language,
- the product derivative,
- the content of the configuration setting “server root path”,
- the ID of the supplier,
- a unique ID for the update check process itself, which is added for reasons of
- security.

This information is SSL encrypted in its entirety and serves solely technical purposes. No personal data or captured data from the system is ever transmitted.

If you do not agree to the transfer of the above-mentioned information, this function can be deactivated in the system settings (“System Settings/evasys Settings/Maintenance/ Automatic Update Check”). Independent of this function, you will be informed of available updates through other channels.

If the administrator uses a secure https connection to the server and if the main server path in evasys is also defined for https (like https://example.com/evasys) and a secure certificate is not installed on the server, the update check will not function.

As the use of non-secure certificates can cause also problems at other sites, and browsers generally recommend not connecting to a server with an unsecure certificate, it is highly recommended to acquire a secure certificate. You will usually get further information on the certificates of your organization from your IT department.

4.4. Client Installation

A special form of the evasys installation is the so-called Client System (tenant based systems). Further subsystem installations are conducted on an (existing) basis system, so that several organizations can evaluate by using a common technical infrastructure.

The server side of the client system possess its own database as well as its own web server address for each client system. In this way, every client has its own data basis, its own settings and its own user administration.

Seen technically, all clients utilize one and the same form evaluation software and therefore all processes must be administered on an inter-client basis. This happens via a master database. The master database administrator (server supervisor) can access all processes which, for reasons of ambiguous identification, could not be allocated to any client. For this reason, the administrator of the main system takes on a role beyond client limits.

The following security features are given:

- The clients are protected from one another. After a successful login, even with knowledge of the web address of other clients, a login cannot be surreptitiously obtained.
- The database access data are encrypted, so that even the server supervisor cannot access the survey data.
- Each client can define own IP address ranges so that external personnel cannot login to the client system, even though it is located physically in another network.
- The images of open questions exist in the file system of the server and can theoretically be seen by the server supervisor. This is why the server supervisor holds a position of trust as well.
- Archiving the digital images from scanned questionnaires can take place directly in the corresponding scanstation. Should the scanstation be positioned decentralized, the archiving will also take place decentralized.

4.5. Hosted Servers

If the evasys system is provided on a server which is operated and maintained by evasys GmbH (so-called “Hosting”), an “Agreement about Collection, Processing or Use of Personal Data on Behalf of Others” (according Article 15 GDPR) can be requested by the customer.

Evasys GmbH requests such an agreement for every third-party company which provides server for evasys hosting.

All servers which are used for hosting purposes are located in Germany.

B. Operational Security in evasys

1. Introduction

In this part of the document, the security of evasys is described regarding undesirable input and the configuration of the web server.

2. Measures to Seal off the Server

- The evasys server is only addressable from the directory /evasys.
- Evasys creates absolute links to the address given in the system.
- The web folder of the webserver cannot be seen and is protected from outside access.
- Access to the MySQL server is only possible via "localhost", SQL requests from other systems within the network are not allowed. Exception: If the database is found on a different server, then precisely the additional IP is allowed. The customer has control over access and is responsible for this control when installing the evasys database onto a MS SQL server.
- The customer is responsible for the secure configuration of the webserver.
- Communication with the server can be operated over a completely encrypted (SSL) connection, for the actual users as well as the online participants.
- All http and https access is logged and can be analyzed with established tools, i.e. for access statistics.
- Secure passwords: During the creation of a password an estimate for the security level will show up. Additionally, a password policy can be enforced. If activated, passwords can only be saved, if they match the following password policy:
    - Length: Min. 8 characters
    - Characters contained: At least one capital letter, one small letter and one number
    - Structure: Not more than two consecutive identical characters

3. Updating Server Components

Evasys GmbH is responsible for the updating of installed applications like MySQL and PHP. Evasys GmbH receives information from the applications manufacturers, so as to provide security updates as soon as possible.

MSSQL and webserver (Internet Information Server, IIS) provided by the customer must also be serviced by the customer, as they can neither be installed nor serviced by evasys GmbH.

4. Measures against Standard Attacks

4.1. Cross-Site-Scripting

The transmitted parameters (GET and POST) are filtered according to <script>. In this way it is prevented, that executable JavaScript code can enter the system or be transferred to the database. JavaScript commands themselves are not filtered, as they pose no threat.

4.2. SQL-Injection

SQL commands transmitted with input fields are not executed, because special characters are masked by relevant measures. In this way, a SQL command transmitted via an input field cannot be executed.

4.3. Penetration test

In 2016, evasys was subject to an extended penetration test by an external security company. A typical evasys installation using an IIS web server was used as testing environment. The test series was not limited to the application, but the entire server was tested with all services. This was done in order to identify incorrect port releases or other critical settings.

In the further course of the test series, the focus has been set on typical security-critical areas and possible vectors of attack, such as code execution, SQL injection, cross-site scripting (XSS), information disclosure, security of authentication and session as well as cross-site request forgery (CSFR) which apply to the common operating of evasys in browsers.

A special test area was also the web service interface (SOAP API), which is decisive for the connection to external systems.

The test series was carried out by the company "SektionEins" (https://www.sektioneins.de/). The results of the tests have been incorporated into the development of the current version.

5. Filtering Undesirable Input

5.1. Filtering in General

Special characters transmitted by input fields are masked, to counteract standard attacks. Beyond this, transmitted tags like, for example, <script> are as a rule filtered or suppressed by masking.

5.2. Filtering in Online Surveys

All HTML tags in the values transmitted are filtered out. The parameters (GET) transmitted over the URL cannot be used to compromise the data base or to execute damaging code. Attempts to overcome the log in of online surveys with SQL injection remain without consequence. No detailed information of the database is shown.