

Data Protection Policy

1. Introduction

When you use our services, you're trusting us with your information. At the Crises Research Centre (CRC), we care greatly about your privacy. We understand this is a big responsibility and work hard to protect your information and put you in control. Our high standards and strong controls for information security allow us to protect your critical and sensitive personal data contained in our information systems. As such, we prevent your personal data from being compromised, altered, lost, destroyed, published or disclosed without proper authorisation.

In order to protect the security and confidentiality of your data, we have developed our Data Protection Policy with the professional help and continuous support of our suppliers-Processors (see below). This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective May 25, 2018

2. Who has access?

Controller

The Controller of your data in the CRC databases is the Crises Research Centre, Eiveniu str. 4 – 512, Kaunas, LT – 50161, Lithuania, Tel. [+370 676 22222](tel:+37067622222), info@smp.lt, registered in Lithuania under company number 134637880.

Processors

The CRC relies on the continuous support of the Processors as listed in Attachment (1). The CRC has agreements with these Processors (art. 28-29 GDPR Regulation) and is supervising that these Processors comply with the GDPR Regulations.

Third parties – Recipients

Neither the Controller, nor the Processor are involved in selling personal data of their users to third parties. In order to provide certain contractually agreed services in the context of the CRC applications, the Processor has recruited the third party services as listed in Attachment (2) as Recipients for the given purposes and may have to share personal data with such third parties. These third parties are authorised to process personal data for the stated purposes and within the given limitations. In case of transfer of personal data to a third country, such access is only granted upon the adequacy decision of the Commission or the appropriate or suitable safeguards as specified in art. 45-46 GDPR Regulation.

Yourself (the Data Subject)

Each registered person can visualise his data by logging in on myhybridlab.com. You can update most of the user data in your account; for corrections of names however the Controller may ask for additional supporting documentation.

Commitments regarding partners of the CRC

All suppliers are thoroughly vetted before being engaged by the CRC for their services. Compliance with applicable data protection legislation (including GDPR compliance) is included in the vetting requirements for all such suppliers. The collaboration with suppliers and the conditions of that collaboration are annually reviewed, including continued compliance with any applicable legal and regulatory requirements. Collaboration may be ceased when a supplier no longer meets such requirements.

To the extent permitted by applicable law, the Controller or the Processor may also disclose your personal data to the following parties:

- Governmental/regulatory authorities and law enforcement agencies.
- (Internal/external) auditors.
- In response to subpoenas, court orders, or other legal, regulatory or judiciary process; to establish or exercise the legal rights of the Controller or the Processor; to defend against legal claims; or as otherwise required by law or binding order.
- When the Controller or the Processor believes it is necessary to investigate, prevent, or take action regarding illegal activities; to protect and defend the rights, property, or safety of Processors, their users, or others.
- In connection with a corporate transaction, such as divestiture, merger, consolidation, or asset sale, or in the unlikely event of bankruptcy.
- With affiliates of the Controller or the Processor.
- The Controller or the Processors may ONLY share aggregated or anonymous information with third parties, including partners, advertisers and investors.

3. What do we process and why?

Data is processed for the legal reason of the legitimate interests. During the design process of the applications, the Controller compiled a data inventory. We intend to acquire and process only the data that is strictly necessary for fulfilling the purposes described below.

Attachment (3) lists the information that can be collected (updated annually), and their interests/purposes.

If you wish to consult the detailed data inventory or wish to acquire more information about the purpose of the data processing activities, please contact the DPO.

4. How long do we store personal data?

As required by applicable data protection legislation, the Controller strives to remove your personal data as soon as it is no longer necessary to accomplish the purpose for which it was originally collected. In view of this principle, the following retention periods apply (executed on an annual basis):

- Courses and certificates data: anonymisation 5 years after the expiry date of a certain qualification (is kept: country, appraisal result, year of birth, profession).
- Membership data: anonymisation 5 years after the last membership date (is kept: country, year of birth, profession)
- Accounting data: information older than 10 years is deleted.
- Personal data: anonymisation 5 years after last login (is kept: country, year of birth, profession, courses/certificates data (see above), membership data (see above)).
- Support questions: removal 2 years after closing support ticket.
- The data will be fully removed from the backups within 180 days after the backup.

5. How do we ensure security?

5.1 Security by design

The following security measures have been implemented to help protect personal data processed through our applications against unauthorized access, alteration, loss, or destruction (non-exhaustive list):

- All data is encrypted both at rest and in transit (check) between the service and your browser.
- Personal data is only accessible after logging in with a personal – unique username and password.
- Passwords are not visible and are neither communicated via email, nor accessible to any person, including Processor's staff.
- All data is fully backed up.
- Actions in your personal data are logged with the identity of the person performing the action, the time stamp and the IP address.
- We do not provide export facilities of user data to recipients; only Course Centres are capable of producing an export of course participants of a certain course with the purpose of sending course information.

5.2 Personal data breach

In the case of a personal data breach that may be a risk to your rights and freedoms, the Controller shall also – within 72 hours after having become aware of it – notify the supervisory authority (Described in art. 55 GDPR Regulation).

In case of a high risk – and without prejudice to the provisions of art. 34, paragraph 3 GDPR Regulation - the Controller will notify you about such personal data breach, with information about the nature, the likely consequences and a contact point for further information.

6. What are your rights as a Data Subject?

Unless your request is reasonably deemed excessive or unfounded, you may exercise the following rights in relation to your personal data processed through our applications:

- Request information concerning the processing of your personal data.
- Request the Controller to modify or correct your personal data if it is wrong.
- Have your personal data erased in certain circumstances as specified under applicable data protection legislation.
- Request the restriction of certain processing activities in certain circumstances as specified under applicable data protection legislation.
- Request a copy of all your data in possession of the Controller and the Processor in a standard format, as well as request for data portability.
- Withdraw your consent.

For a full review of your rights as Data Subject, please consult the General Data Protection Regulation.

You can easily exercise any of your rights by completing and submitting our online form. The Controller reserves the right to charge a reasonable fee in case your request is deemed excessive at our sole discretion.

6.1 Modifying and correcting your personal data (rectification)

HybridLab allows Data Subjects to manage the processed personal data themselves. If you are unable to complete the modifications or corrections to the data, then you can request the Controller to perform this action by submitting a request to myhybridlab.com.

6.2 Removing your personal data

The following procedure will be applied when a request for removal of data from the Data Subject is presented to the CRC:

Because of the irreversibility of such action, in order to request a removal of personal data, the Data Subject must submit such request by logging in on myhybridlab.com and include a copy of their ID/Passport for identification purposes. The Controller may send an email reply first to check the authenticity of the request.

The Controller will assess without undue delay the nature of the request and check which data need to be removed from which database in accordance with the GDPR requirements. If the personal data is present in the application, the Controller will remove the personal data from the database of the application/system and apply the anonymisation procedures within 30 calendar days following the personal data removal request. The Controller notifies (by email) the Data Subject about removal within 30 calendar days. If the Controller cannot grant the request for removal, the DPO will notify the Data Subject about such decision and the motivation within 30 days following the data removal request.

All personal data that you have selected for deletion will be fully purged from the backups within 180 days.

WARNING: removing personal data may lead to irreversibly losing any personal link or trace of membership, trainings, certificates or qualifications. The controller however will keep a printed record of the request of removal for reasons of proof and Controller's liability. Such printed records will not be processed by automated means and neither in a filing system or with the intention to form part of a filing system, hence the GDPR regulation does not apply (Art. 2, paragraph 1 GDPR Regulation).

6.3 Apply restrictions of certain processing activities

A dedicated myhybridlab.com page in the Data Subject's account gives the possibility to subscribe or unsubscribe individually from the different newsletters, groups and other communication types. Changes made by the Data Subject are applied within one week at the latest.

Unsubscribing from emails containing news facts, event or services provided by the can alternatively be executed by using the unsubscribe button or hyperlink included in every newsletter or group email.

However, when registered for a course and until the course is closed administratively, identity and contact details are shared with the Course Centre. As a Course Centre cannot run a course without the possibility to contact the participants, this permission is mandatory in order to register for a course.

6.4 Receive a copy of all your data – data portability

Attachment (1) lists how a Data Subject can create an overview of all available data in the Controller's (Processor's) systems.

The Data Subject can apply for an export in an electronic format of his personal data and qualifications, for data portability purposes. The Controller is not responsible for the format of this data in order to be uploaded in other systems.

6.5 Withdraw your consent

You have the right to withdraw your consent at any time. However, such withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.

7. How you can provide consent?

By accepting this privacy statement and furnishing personal data via myhybridlab.com, you expressly give consent to the Controller to process the data for the stated purposes.

Only upon your individual consent, the Controller will pass on specific personal data to third parties. The foregoing also applies to processing of personal data outside of the EU, both in countries or recognised and not recognised by the European Commission to offer adequate data protection. Where required, a data transfer agreement will be entered into, in accordance with the contractual clauses set out in EU Commission Decision C(2010)593 Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC).

8. Who can you contact?

If you have any questions about this privacy policy, or if you want to exercise any of the Data Subject rights stipulated above, please contact the Controller on info@myhybridlab.com

Data Policy CRC - Attachment 1

List of Processors

The following natural or legal persons, public authorities, agencies or other bodies, process* personal data on behalf of the Controller (art. 4, 8 GDPR Regulation).

Processor	Purpose(s)	Data copy	Contact
Navision	Accounting	Customers can ask for a copy of the invoices created.	www.dynamics.microsoft.com/en-us/nav-overview
Zendesk Chat	Customer support system	You can access the Support system via myhybridlab.com and ask (if you need) for a copy of the communication.	www.zopim.com
Totara	Course content E-learning Personal data database Course administration Web shop	You can print the available pages with collected data. Also you can create a printed report of personal data, qualifications and course history.	www.totarlms.com
Mailgun	User mailings	Mail addresses are stored according to the groups the Data Subject belongs.	www.mailgun.com
ExtLMS	Translation management Management of simulation training Creation and development of training material	Translators can ask info@myhybridlab.com for a report of their activities as a translator. You can print the available pages with collected data related to simulation and training material.	www.lms.myhybridlab.com
PowerBI	Data Analysis Tool	Data is stored and used for statistical analysis of training parameters.	powerbi.microsoft.com

Jira	Issue tracking system	Personal data might be temporary stored in Jira if necessary to improve MYHYBRIDLAB.	www.atlassian.com
G Suite	E-mail client (Gmail) Office programs (Google Docs) Online storage (Google Drive) Calendar Communication platform (Hangout)	Communications and office documents with customer's personal data are stored for 2 years.	www.google.com
Microsoft Office	Office programs	Office documents with customer's personal data are stored for 2 years.	www.microsoft.com
Solink	Video data for course evaluation	Video data is used to identify the person in the courses, course appraisal purposes and quality assurance.	solinkcloud.com
Dahua Smart PSS	Video data for course evaluation	Video data is used to identify the person in the courses, course appraisal purposes and quality assurance.	www.dahuasecurity.com

* 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

Data Policy CRC - Attachment 2

List of Recipients

To the following natural or legal persons, public authorities, agencies or other bodies, personal data is disclosed, whether a third party or not (art. 4, 9 GDPR Regulation).

Recipients	Purpose(s)	Limitations
ERC (European Resuscitation Council)	Quality Control of courses	Access to individual accounts of their users. Access to course data within their country. No export tools.
AHA (American Heart Association)	Quality Control of courses	Access to individual accounts of their users. Access to course data within their country. No export tools.
American College of Surgeons	Quality Control of courses	Access to individual accounts of their users. Access to course data within their country. No export tools.
ALSG (Advanced Life Support Group)	Quality Control of courses	Access to individual accounts of their users. Access to course data within their country. No export tools.
AAFP (American Academy of family physicians)	Quality Control of courses	Access to individual accounts of their users. Access to course data within their country. No export tools.
Course instructors	Quality control of courses	Access to individual accounts of participants for the courses. Access to course data for their relevant course types. No export tools.
Course Centres	Administration of courses	Access to personal data either by mandate of, or upon explicit (but mandatory) approval by the course participant. Export of address details on a course level is facilitated, in order to ship paper manuals (to the extent supported).
Course Director	Certification of participants	Access to personal data related to the Course Centre's permissions of access. No export tools.

Data Policy CRC - Attachment 3
Information collected by the Controller for which interests

Data type	Interest/purpose	Mandatory
First name/Surname	Uniquely identify persons	Yes
Additional names (First name – phonetic, Surname – phonetic, Middle name, Alternate name)	Notification Templates for message personalization	No
Username	Uniquely identify persons	No
Email address	Communication with users (Data Subjects) Feedback Unique identifier	For specific groups ¹
Email display	Communication with users (Data Subjects)	No ²
Gender (sex)	Statistical purposes	No
Date of birth	Avoid double records	Yes
Personal number	Uniquely identify persons	No
Country	Statistical purposes	No
County, Municipality, City/town	Statistical purposes Delivery of goods	Yes
Address	Delivery of goods	Yes
Postal code	Delivery of goods	No
Time zone	Statistical purposes Training purposes	No
Phone	Communication with users (Data Subjects) Feedback Unique identifier	Yes
Mobile, Additional phone, Fax no., Web page, Work phone	Communication with users (Data Subjects) Unique identifier	No
Organization, department, position	Statistical purposes	No
Job standing, Last job standing	Statistical purposes	No
Education (Institution, Diploma no., Diploma specialty, Diploma issue date, Diploma serial no., License no., License issue date, License serial no.)	Statistical purposes	No
User picture	Identify the person in the courses	No
List of interests	Statistical purposes	No
Aspirational position	Statistical purposes	No
Skype ID	Statistical purposes	No
Password	Login security	Yes
New password	Login security	No
Preferred language	Presenting information in a familiar language	No
Membership history	Statistical purposes	No

Courses history	Certificate justification User feedback and quality control on trainings	Yes
Course appraisal results	Creation of Certificates Statistical purposes	Yes ¹
Certificates status	Certificate justification Delivery of certificates and recertification	Yes
Registry of orders	Complete pending orders Provide an overview of past orders as a service to the customers	Yes
Event place and history	Visualize events managed by the Controller	Yes
Course Survey data	Quality control of courses	Yes
Video data	Identify the person in the courses Course appraisal purposes and quality assurance To ensure the chosen teaching method. Video surveillance allows you to evaluate the training process for a larger number of experts. Do not cause additional stress in training for participants. Trainers and instructors have the opportunity to monitor, evaluate and correct their actions.	Yes

¹Instructors, Instructor Candidates, Coordinators, Course Directors, Educators.

²Additionally the Data Subject can choose to share or not his e-mail with course members.