PRIVACY POLICY

1.2.

Data Controller: Nitrolearning Zrt.

Registered office: 1119 Budapest, Andor utca 21/c. fszt. 1.

Correspondence address and the address of administration: 1119 Budapest, Andor utca 21/c. fszt. 1.

Telephone number: +36 20 288 66 27

E-mail: info@nitrolearning.hu

Last modified: 17th April 2023

TABLE OF CONTENT

1. GENERAL INFORMATION

Purpose of the Privacy Policy:

Nitrolearning Zrt. (hereinafter referred to as Nitrolearning) processes personal data as a Data Controller and a Data Processor regarding those data subjects that get in touch with the software and the related services directly as a Subscriber – the contact person of the Subscriber – or indirectly as users invited by the Subscriber.

The purpose of the provisions and conditions set out in this Policy – pursuant to the effective data protection law – is to determine the frameworks of the data processing carried out by the Data Controller and to inform all the data subjects on the details of the processing of the personal data provided by them or via any intermediary parties. Another purpose of the Policy is to provide the data subjects with short, concise, and clear information prior to the provision of personal data about the purposes for which the software and services process and store their personal data, on what legal basis, under what conditions and subject to what safeguards, and for how long. Beyond the above, the Policy provides information on the rights of the data subjects related to the data processing, the responsibilities of the Data Controller, the Data Processors invited by the Data Controller and the authorities to which the data subjects can turn to in the course of exercising their rights.

Following prior notification, the Data Controller shall be entitled to amend this Policy pursuant to the appicable law and in accordance to the changes in the software and the related services. If you use the software or visit our website, we recommend you to find information on the amendments of the Privacy Policy irrespective of the notifications.

Before using the Courze&Cloud software or the related services, please, read the following Policy carefully, and contact our colleagues engaged in data processing if you have any questions or comments in relation to this Privacy Policy.

Phone: +36 305828287

E-mail address: jog@nitrolearning.hu

Purpose of the Courze&Cloud software and the services:

Courze&Cloud is such a framework, which provides a simpler and more user-friendly way for the Subscriber and the users invited by the Subscriber to create, store, publish, and play e-learning material than the other opportunities available on the market. The Courze&Cloud softver identifies 3 roles:

Organization administrator: has access to the settings of the organization, and manages the further users' access.

Editor of the learning material: has the right to create learning material, can add content to it, edit it and publish the learning material.

Student: has the right to view the learning material shared to him/her.

Learning material editing service

The learning material editing service provides an opportunity to create, edit, modify, delete and publish the learning material (and its content).

Learning material player service

The learning material player service provides an opportunity to display any learning material published in the Courze&Cloud player service and to follow up on the students' performance.

2. INFORMATION FOR THE USERS

The Courze&Cloud software, and the related services, have been designed to satisfy the needs of economic entities and organizations (hereinafter jointly referred to as Subscriber) and it is not intended for private people.

If the Subscriber makes the use of the software and the related services available to you – in particular, but not exclusively as your employer –, the administrator's duties over your user account must be performed by the Subscriber, and it will exercise the administrator rights as well. In this respect, the Subscriber shall be deemed as the Data Controller, and Nitrolearning Zrt. participates in the performance of data processing as the Data Processor. **Nitrolearning Zrt. shall not be liable to the data protection and data security policies applied by the Subscriber as well as for the implemented measures which might be different from the below rules of data protection and data security.**

3. AMENDMENT AND REVISION OF THE POLICY

Considering that this Policy is part of the Service Regulations related to the services, the Data Controller reserves the right to amend this Policy unilateraly. Please, follow up on the website regularly to get up-to-date information about the potential amendments. Beyond the above, the Data Controller shall publish any amendments at least 15 days prior to its entry into force.

4. RELEVANT LEGAL REGULATIONS

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive (EC) No 95/46 (hereinafter referred to as **GDPR**);

Act CXII of 2011 on the right of informational self-determination and on freedom of information (hereinafter referred to as **Infotv.**);

Act V of 2013 on the Hungarian Civil Code (hereinafter referred to as **Ptk.**)

Act CVIII of 2001 on electronic commerce and on information society services (hereinafter referred to as **Elkertv.**)

5. CONCEPTS IN RELATION TO DATA PROCESSING

GDPR shall define the definitions used during the processing of personal data. For the sake of transparency and clarity, the Data Controller takes out the most important concepts in this section from the GDPR.

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. **"Sensitive data"** means the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Generally, the processing of this data is prohibited.
3. **"Data processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not performed by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
4. **"Restriction of processing"** means the marking of stored personal data with the aim of limiting their processing in the future.
5. **"Data Controller"** means the natural person or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
6. **"Data Processor"** means a natural person or legal entity, public authority, agency or other body which processes personal data on behalf of the controller.

7. **"Recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
8. **"Third party**" means a natural person or legal entity, public authority, agency or body other than the data subject, data controller, data processor and persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.
9. **"Consent of the data subject"** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
10. **"Personal data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
11. **"Sevice Provider"** means a legal entity or organization providing services directly to the Subscriber or indirectly to the users via the Subscriber.
12. **"Subscriber"** means a legal entity or organization using the services directly pursuant to an agreement concluded with the Service Provider, which publishes e-learning material to the invited users and in certain cases – on the basis of a separate agreement by and between the Subscriber and the user or the users –, processes data via the Service Provider in relation to the learning material published in its name as well as the users editing and playing them.
13. **"User"** means a person with an editorial and/or student profile specified by the Subscriber, which is entitled to edit and/or play the accessed learning material pursuant to the level of authorization.
14. **"Supervising authority"** means an independent public authority founded by a member state in accordance with article 51 of the GDPR.
15. **Tenant**: An account created by Nitrolearning for individual subscribers, featuring a separate data area.

6. PROCESSING OF DATA AS A DATA CONTROLLER

6.1. Filling out the form found on the www.courzeandcloud.com website, for the purpose of providing a Courze&Cloud trial account

Activities as a data controller and purpose of data processing: The Data Controller processes the data below for the purpose of providing a trial account and sending the username and temporary password to the data subject.

The legal basis of data processing: The Data Controller processes the data subject's data specified below based on Article 6(1)(f) of the GDPR, on the legitimate interest of the Data Controller to provide specified services to the data subject for a defined period.

The scope of data subjects: Individuals who complete the form.

The processed personal data:

- name of the natural person;
- business email address;
- phone number.

Duration of data processing: The Data Controller processes the above-defined data until the username and password required for accessing the trial account are sent and then deletes them within 30 days.

The Data Controller uses the following data processor for storing the data.
The Data Controller does not transfer the personal data specified above to a third country or an international organization.

Name	Registered office	Task of the Data Processor
Microsoft Forms	South County	https://www.microsoft.com/hu-

	Business Park Leopardstown Dublin 18, D18 P521, Ireland	hu/servicesagreement/default.aspx

The rights of data subjects: the data subject may
a) request information about the processing of the personal data and access the processed personal data;
b) request the rectification of the personal data,
c) request the erasure of the personal data,
d) request the limitation of the processing of the personal data,
e) object to the processing of the personal data,
f) exercise the right to data portability,
g) exercise the right to remedy.

In accordance to the information at the end of this document, the data subject may lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) or the competent court.

6.2. Courze&Cloud demo appointment booking

Activities as a data controller and purpose of data processing: In order to hold a demo for the data subject, the Data Controller provides a registration and appointment booking opportunity on an interface provided by Calendly (data processor).

The legal basis of data processing: The Data Controller processes the data specified below of the data subject based on the legitimate interest of the Data Controller, pursuant to Article 6 (1) (f) of the GDPR, to provide specified services for a specified period.

The scope of data subjects: Individuals who book an appointment in the Calendly application and provide their data below.

The processed personal data:

- name of the natural person (name provided by the data subject);
- email address;

Duration of data processing: The Data Controller processes the above-specified data for the purpose of booking the demo appointment, and the personal data will be deleted in accordance with the data storage and deletion rules of third parties.

The Data Controller uses the following data processor for storing the data:

Name	Registered office	Task of the Data Processor
Calendly	Calendly LLC115 E Main St., Ste A1BBuford, GA 30518 USA/ DPO Centre Europe, BERLIN: Friedrichstrabe 88, Excellent Business Centre, Berlin, 10117, Germany	Synchronization of calendar applications used by the Data Controller and data subjects.

The application operated by the data processor is connected to other calendar applications managed by third parties, which it synchronizes on a single platform. As a result, the data entered by the data subject on the interface

provided by the Data Controller is synchronized in both the data subject's and the Data Controller's calendar applications.
If you need more information:
https://calendly.com/dpa

The rights of data subjects: the data subject may
a) request information about the processing of the personal data and access the processed personal data;
b) request the rectification of the personal data,
c) request the erasure of the personal data,
d) request the limitation of the processing of the personal data,
e) object to the processing of the personal data,
f) exercise the right to data portability,
g) exercise the right to remedy.

In accordance to the information at the end of this document, the data subject may lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) or the competent court.

6.3. Registration and management of the subscriber's administrator account

Activities as a Data Controller: Performance of the operations related to the creation (registration) of a subscriber's administration account, contact The registration makes the use of the software and the services possible.

The purpose of data processing: To create the circumstances necessary for the use of the software and the services. It requires an administrator account.

The legal basis of data processing: The Data Controller processes the personal data of the data subject specified below in accordance to Article 6 (1) f) of the GDPR in favour of the contractual performance of the Service Agreement concluded with the Subscriber.

The scope of data subjects: Those people who manages the Subscriber's administrator account.

The processed personal data:

- e-mail address
- password associated to the e-mail address

Duration of data processing: The Data Controller processes the above data until the termination of the Service Agreement concluded with the Subscriber.

The Data Controller shall not transfer the above data to any third countries or international organizations.

The rights of data subjects: the data subject may
a) request information about the processing of the personal data and access the processed personal data;
b) request the rectification of the personal data,
c) request the erasure of the personal data,
d) request the limitation of the processing of the personal data,
e) object to the processing of the personal data,
f) exercise the right to data portability,
g) exercise the right to remedy.

In accordance to the information at the end of this document, the data subject may lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) or the competent court.

6.4. Data processing in relation to the user account

Activities as a Data Controller: The verification in relation to the user account and its creation

The purpose of data processing: To verify which subscriber created the account or under which subscription the account was created.

The legal basis of data processing: The Data Controller processes the personal data of the data subject specified below in accordance to Article 6 (1) f) of the GDPR based on the provisions of the Service Agreement concluded with the Subscriber, considering that the number of accounts created by the Subscriber or in the framework of the subscription is clearly determined in the Service Agreement. Finally, the Data Controller verifies the contractual performance of the Service Agreement on the side of the Subscriber.

The scope of data subjects: The data subjects in whose name the Subscriber creates a user profile, or who created a user profile in the framework of the Subscription.

The processed personal data:

- e-mail address
- password associated to the e-mail address
- editorial/student authorization
- belonging to the Subscriber

Duration of data processing: The Data Controller processes the above data until the termination of the Service Agreement concluded with the Subscriber.

The Data Controller shall not transfer the above data to any third countries or international organizations.

The rights of data subjects: the data subject may
a) request information about the processing of the personal data and access the processed personal data;
b) request the rectification of the personal data,
c) request the erasure of the personal data,
d) request the limitation of the processing of the personal data,
e) object to the processing of the personal data,
f) exercise the right to data portability,
g) exercise the right to remedy.

In accordance to the information at the end of this document, the data subject may lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) or go to the competent court.

6.5. Subsciption to the newsletter, sending the newsletter

Activities as a Data Controller: Information of the subscribers and the potential new clients

The purpose of data processing: Notification of the Courze&Cloud and its related services as well as the new products, news and potential discounts related to the other services of Nitrolearning Zrt.

The legal basis of data processing: The Data Controller processes the personal data of the data subject specified below in accordance to Article 6 (1) a) of the GDPR in favour of receiving the voluntary, specified, information-based and clear consent by the data subject which is necessary for the use of the service.

The scope of data subjects: The data subjects who have explicitly indicated that they want to use the service.

The processed personal data:

- e-mail address
- name (optional)

Duration of data processing: Until the withdrawal of the consent, unsubscription from the newsletter or the termination of the service by the Data Controller.

The Data Controller shall not transfer the above data to any third countries or international organizations.

You can easily unsubscribe from the newsletter by clicking on the "Unsubscribe" button at the bottom of the newsletter.

The consequences of the absence of consent: The newsletter is only sent to those who have expressly subscribed to the service based on their free will.

The rights of data subjects: the data subject may
a) request information about the processing of the personal data and access the processed personal data;
b) request the rectification of the personal data,
c) request the erasure of the personal data,
d) request the limitation of the processing of the personal data,
e) object to the processing of the personal data,
f) exercise the right to data portability,
g) exercise the right to remedy.

In accordance to the information at the end of this document, the data subject may lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) or go to the competent court.

6.6. Management of errors, complaints or questions submitted by the Subscriber or the user (Support, Helpdesk)

Activities as a Data Controller: Operation of the support and helpdesk attributed to the software and the related services

The purpose of data processing: The management of errors, complaints and reports of other kinds considering the software and the related services and submitted by the administrator of the scubscriber's account and/or the data subjects having user accounts

The legal basis of data processing: The Data Controller processes the personal data of the data subject specified below in accordance to Article 6 (1) f) of the GDPR in favour of the contractual performance of the provisions of the Service Agreement and the Service Level Agreement concluded with the Subscriber, the trouble-free operation of the software and its further development.

The scope of data subjects: The data subjects managing a subscriber's account or having a user account and submitting any errors to the support or the helpdesk

The processed personal data:

- e-mail address
- password associated to the e-mail address

- the problem, error or report submitted in relation to the software or the services[1]

Duration of data processing: The Data Controller processes the above data until the resolution of the error or problem, the processing of the report or the end of its resolution. If the report, the error or the problem is in relation to the Service Agreement or the relevant Service Level Agreement conclcuded by and between the Subscriber and the Service Provider and the prevention of the error or the probems is required for the contractual performance by the Data Controller, the term of data processing shall be aligned with to the term of the Service Agreement between the Subscriber and the Service Provider.

The Data Controller shall not transfer the above data to any third countries or international organizations.

The rights of data subjects: the data subject may
a) request information about the processing of the personal data and access the processed personal data;
b) request the rectification of the personal data,
c) request the erasure of the personal data,
d) request the limitation of the processing of the personal data,
e) object to the processing of the personal data,
f) exercise the right to data portability,
g) exercise the right to remedy.

In accordance to the information at the end of this document, the data subject may lodge a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) or go to the competent court.

7. DATA PROCESSING AS A DATA PROCESSOR

Nitrolearning acts as a Data Processor in any actions of data processing processor - except for those explicitly identifying xxx as a data controller in the table below - in which the Subscriber publishes their own learning material via the C&C software, i.e. makes it available to their users. In the above case, the Subscriber, as a data controller, determines the purposes and methods of using the data they wish to process, and xxxx, as a data processor, participates in the data processing operations.

Data in relation to the student and editorial activity that the Subscriber, as Data Controller, may process in accordance with the legitimate purpose or purposes and legal basis specified by the Subscriber and that Nitrolearning, as Data Processor, may provide to the Subscriber.

In addition to the above, Nitrolearning processes personal data related to user (learner/editor) activities as follows:
The user, who:
- opened any learning material;
- opened a page within any learning material;
- displayed any widget on the screen;
- interacted with a widget (e.g. by turning a learning card, or playing a video);

The user, in respect of whom
- the performance of a widget is completed;
- the performance of a page is completed;
- the performance of any learning material is completed;

1 It may happen that a report submitted by a data subject includes specific personal data of specific data subjects and gets processed by the Data Controller.

Summary of personal data processing (in the case of the following data processing operations, the legal basis is Article 6(1)(f) of the GDPR, based on Nitrolearning's legitimate interest in ensuring the use of the software in accordance with the provisions of the service contract concluded with the Subscriber, so that it is smooth and secure. In this regard, where the operation requires more precise specification, we indicate it separately.):

Personal data processed	Mandatory or not?	What is the purpose of the data processing?	Legal basis of processing	The duration of processing
System administrators and editors (those who have access to back-office systems, such as course editing, exam editing, etc.)				
First name + last name	yes	In order to accurately determine who is using the services/ whose data we processing.	GDPR Article 6 (1)(f), For the purpose of preventing abuse and identifying the tenant	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
e-mail address	yes	We use this to identify the data subject. Furthermore, we can send a forgotten password to them this way, and system messages will also be sent to this address.	GDPR Article 6 (1)(f), For identification and replacing forgotten passwords, as well as sending system and other messages related to the software.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Password	yes	With this, as above identify the user, allowing them to securely access the system.	GDPR Article 6 (1)(f), To ensure proper protection of the account and ultimately the software.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
FB account conneciton	no	Only if it is allowed in the given tenant and the user has logged in with it.	GDPR Article 6 (1)(f), To offer a more complete user experience. This simplifies the login process, for which the individual makes the decision, and the system only facilitates it.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Google account connection	no	Only if it is allowed in the given tenant and the user has logged in with it.	GDPR Article 6 (1)(f), To offer a more complete user experience. This	until the user is deleted (for example: Subscriber wants the user deleted, or Service

			simplifies the login process, for which the individual makes the decision, and the system only facilitates it.	Agreement terminated)
Two-factor authentication	no	Only if it is allowed in the given tenant and the user has logged in using it.	GDPR Article 6 (1)(f), For security reasons, the software grants it based on the individual's choice.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Language	yes	This way, we know in which language to display the software.	GDPR Article 6 (1)(f), for better user experience and easier manageability.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Audit log about user activity	yes	This way, activities that have taken place in the system can be traced back. It is possible to see who did what and when. Any potential abuse (such as deleting course material) can be traced back.	GDPR Article 6 (1)(f), n order to prevent abuses, breaches of contract, and ultimately to protect the software and its subscribers, as well as to ensure that users comply with the obligations set out in the General Terms and Conditions.	1 hónap-30 nap in case of any problems, it can be retrievable within this timeframe. This is approximately when the issue is usually detected and a procedure can begin to investigate.
which learning materials did the user created	yes	In regards to their self-created learning materials, everyone has special rights therefore it is necessary to keep track of who the creator of a course material is."	GDPR Article 6 (1)(f), Enforcing the goals set forth, ensuring user rights and entitlements.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
which exams did the user created	yes	In regards to their self-created exams everyone has special rights therefore it is necessary to keep track of who the creator of an exam is	GDPR Article 6 (1)(f), Enforcing the goals set forth, ensuring user rights and entitlements.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)

In which learning materials is a user a co-editor	yes	Access must also be provided for these learning materials.	GDPR Article 6 (1)(f), Enforcing the goals set forth, ensuring user rights and entitlements.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Roles	yes	This describes the functions that the given user is authorized to access within the system (e.g. system administrator, course editor, exam editor, lead course editor).	GDPR Article 6 (1)(f), Enforcing the set goals and obligations, ensuring user rights and entitlements.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Identity Service Provider ID	setting dependent	It is possible that some other system determines who can log in to the system (e.g. LDAP, AD, or some SSO). In this case, it is stored what the identifier of the given user is in that system.	GDPR Article 6 (1)(f), It is necessary for the system to function properly and be used without issues, as well as for user identification.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Students				
First name + last name	yes	In order to accurately determine who is using the services/ whose data we processing.	GDPR Article 6 (1)(f), For the purpose of preventing abuse and identifying the tenant	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
e-mail address	no/setting dependent	We use this to identify the data subject. Furthermore, we can send a forgotten password to them this way, and system messages will also be sent to this address.	GDPR Article 6 (1)(f), For identification and replacing forgotten passwords, as well as sending system and other messages related to the software.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Password	no/setting dependent	With this, as above identify the user, allowing them to securely access the system.	GDPR Article 6 (1)(f), To ensure proper protection of the account and ultimately the software.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)

FB account conneciton	no	Only if it is allowed in the given tenant and the user has logged in with it.	GDPR Article 6 (1)(f), To offer a more complete user experience. This simplifies the login process, for which the individual makes the decision, and the system only facilitates it.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Google account connection	no	Only if it is allowed in the given tenant and the user has logged in with it.	GDPR Article 6 (1)(f), To offer a more complete user experience. This simplifies the login process, for which the individual makes the decision, and the system only facilitates it.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Two-factor authentication	no	Only if it is allowed in the given tenant and the user has logged in using it.	GDPR Article 6 (1)(f), For security reasons, the software grants it based on the individual's choice.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Language	yes	This way, we know in which language to display the software.	GDPR Article 6 (1)(f), for better user experience and easier manageability.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
LTI provider URL	no/setting dependent	If the student arrived through LTI, this is the URL where we can send their results back to the initiating system.	GDPR Article 6 (1)(f), It is necessary for the system to function properly and be used without issues, as well as for user identification.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)
Learning Activities (Interactions)	yes	Accurate recording of the operations a student performs within course material. For example: watched a video, loaded	GDPR Article 6 (1)(f), Recording the data necessary for the student experience	until the tenant is deleted

Learning Record Store - storage of learning activities Data transfer upon data controller's instruction		a page, viewed the solution to a task. Storing this information is necessary in order to determine whether a course material has been completed. Additionally, these data help measure a student's progress.	and the implementation of specific learning methodological principles when completing the course material, so that the content can truly achieve the goals defined by its creators.	
Identity Service Provider ID	setting dependent	It is possible that some other system determines who can log in to the system (e.g. LDAP, AD, or some SSO). In this case, it is stored what the identifier of the given user is in that system.	GDPR Article 6 (1)(f), It is necessary for the system to function properly and be used without issues, as well as for user identification.	until the user is deleted (for example: Subscriber wants the user deleted, or Service Agreement terminated)

8. DATA PROCESSORS

Name	Registered office	Task of the Data Processor
Nitrowise Labs Zrt.	1119 Budapest, Mohai út 38.	Software development, data storage, provision of server capacity
Microsoft Ireland Operations, Ltd.	South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Storage of security backup, Microsoft Azure
Twilio Ireland Limited	3 Dublin Landings, North Wall Quay Dublin 1, Ireland	Hírlevelek, rendszerüzenetek, tranzakciós üzenetek megküldése az előfizetők részére
Infotechna Kft.	1037 Budapest, Zay utca 1-3.	Storage of servers

9. RIGHTS OF THE DATA SUBJECTS IN RELATION TO THE DATA PROCESSING

The Data Controller shall ensure that the rights of data subjects are respected as follows.

The Data cController provides the data subject with opportunity to submit his/her request in relation to the exercise of his/her rights in any of the following ways and via the contact details set out in this Policy: (i) by post, (ii) via e-mail and (iii) by phone.

The Data Controller shall perform the request submitted by the data subject without unreasonable delay, but at last within 30 days of the receipt of the request, and shall provide information to the data subject in a concise, transparent, understandable and easily accessible form in clear and plain language. The Data Controller shall decide about the refusal of the request within the same deadline, and it shall inform the

data subject about the refusal of the request and its reasons as well as the remedies available to the data subject in this regard.

Generally, the Data Controller shall perform the request submitted by the data subject by e-mail, except the data subject requests it otherwise. Information by phone on the request submitted by the data subject may only be given if the data subject verifies his/her personal identity. The Data Controller shall not use the correspondence address or the telephone number of the data subject for any other purposes.

The Data Controller shall not charge any fee or expense to the data subject for the performance of the – below specified – requests. In the event that an unfounded, excessive request for the same set of data is received from the data subject within one year of the previous, already executed request, the Data Controller reserves the right to charge reasonable compensation for executing the request, proportionate to the workload of executing the request, or to refuse to act on the request, in its discretion, giving adequate reasons.

- **The right to information on and access to the personal data**

The Data Controller shall provide information on the request submitted by the data subject in a concise, transparent, understandable and easily accessible form in clear and plain language including the following information:

- whether his/her personal data is being processed by the Data Controller;
- the name and contact details of the Data Controller;
- the fact of data processing and the name and contact details of the Data Processors set out above;
- the personal data of the data subject processed by the Data Controller, and the sources of information;
- the purposes of the date processing as well as its legal basis;
- the term of data processing;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular, recipients in any third countries or international organisations;
- the rights of the data subject;
- the circumstances and the effects of a potential data protection breach, and the measures taken in favour of its prevention.

- **The right to rectification**

Upon the request submitted by the data subject, the Data Controller shall rectify the inaccurate personal data referring to the data subject.

The Data Controller shall inform each recipient on the rectification, to whom the personal data has been disclosed, unless this proves to be impossible or requires disproportionate efforts. Upon the request submitted by the data subject, the Data Controller shall provide information on the scope of the recipients.

- **The right to erasure ("to be forgotten")**

Upon the request submitted by the data subject, the Data Controller shall erase the personal data referring to the data subject where any of the following applies:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the data subject objects to the data processing;
- the personal data have been unlawfully processed by the Data Controller;
- the personal data have to be erased in favour of complying with a legal obligation in Union or Hungarian law to which the Data Controller is subject.

The Data Controller shall inform each recipient on the erasure, to whom the personal data has been disclosed, unless this proves to be impossible or requires disproportionate efforts. Upon the request submitted by the data subject, the Data Controller shall provide information on the scope of the recipients.

- **The right to the restriction of data processing**

Upon the request submitted by the data subject, the Data Controller shall restrict the data processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject – in such cases the restriction applies for a period enabling the Data Controller to verify the accuracy of the personal data;
- the processing is unlawful but the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

The Data Controller shall inform each recipient on the restriction, to whom the personal data has been disclosed, unless this proves to be impossible or requires disproportionate efforts. Upon the request submitted by the data subject, the Data Controller shall provide information on the scope of the recipients.

- **The right to data portability**

Upon the request submitted by the data subject, the Data Controller shall provide the personal data relevant to and provided by the data subject. Moreover, the Data Controller shall undertake that the data subject can transfer this personal data to another data controller without being restricted by the Data Controller.

- **The right to remedy**

If the data subjects believes that the Data Controller breached the data subject's right to the protection of personal data in the course of the data processing, he/she may lodge a complaint at the competent authorities pursuant to the applicable law, i.e. the data subject may lodge a complaint to the NAIH (address: H-1055 Budapest, Falk Miksa utca 9-11.; correspondence address: 1363 Budapest, Pf. 9.; website: www.naih.hu; e-mail address: ugyfelszolgalat@naih.hu; telephone: +36-1/391-1400) or may go the competent court.

The Data Controller hereby undertakes to cooperate with the competent court or the NAIH and provides the competent court or the NAIH with the data related to the processing.

The Data Controller also undertakes to compensate the data subject for the damage caused by the unlawful processing of the personal data or breaching the requirements of data security. The data subject is entitled for a grievance award in the case of the breach of his/her personal rights. The Data Controller shall be exempted from the liability if the damage has been caused by any unavoidable reasons beyond the scope of the data processing, or if the impairment caused by the damage or the breach of the personal rights arose from the deliberate or grossly negligent behaviour of the data subject.

10. MEASUREMENTS OF DATA SECURITY

The Data Controller shall be responsible for ensuring data security. The Data Controller took the necessary technical and organizational measures, and estabished the procedures that ensure the protection of the collected, stored and processed data and avoid its destruction, unathorized use and unauthorized modification. Furthermore, it hereby informs those third parties to whom the data of the data subject has been forwarded that they are obliged to comply with the requirements of data security.

The Data Controller shall avoid the access to, or the disclosure, the transfer, the modification and the erasure of the processed data by any unauthorized people.

The Data Controller shall take all the reasonable measures to avoid the damage or the destruction of the processed personal data. The above commitment is also required by the Data Controller for its employees and partners involved in the data processing activities, including the Data Processors acting on behalf of the Data Controller.

11. MANAGEMENT OF PERSONAL DATA BREACH

If the Data Controller detects the accidental or unlawful destruction, loss, modification, unathorized transfer or disclosure of or any events or acts resulting in the unlawful access to the transferred, stored or otherwised processed personal data (hereinafter referred to as personal data breach), it shall comply with Article 33-34 of the GDPR and report the personal data breach to the competent data protection authority (hereinafter referred to as NAIH), and to inform the data subject or the data subjects of the personal data breach if it probably imposes high level of risk with regard to the rights and freedom of the natural people.

The person, who detects any personal data breaches with regard to the personal data transferred, stored or otherwise processed by the Data Controller, may report it to the Data Controller via the following contact details:

Telefonon: +36 20 288 66 27
E-mail: info@nitrolearning.hu

Beyond the determination of the subject of the personal data breach, the notifier shall provide the below information:

- name of the notifier;
- contact details of the notifier: telephone and/or e-mail address,
- whether the personal data breach affects the software, and if so, which part or which service.

The Data Controller investigates the report within 1 working day, or immediately if it considers the incident as serious, and – if necessary – it request further information from the notifier. Within 72 hours of the report of the personal data breach, the Data Controller provides data to the NAIH.

The reporting shall contain the following data:

- the nature of the personal data breach including the categories and the approximate number of data subjects concerned and the categories and the approximate number of personal data records concerned;
- the name and contact details of the person providing more information;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If the personal data breach requires further investigation, the Data Controller shall take all the necessary measures to assess the real and potential impacts of the personal data breach during the investigation, with the involvement of appropriate experts. The involved experts shall prepare a report about the investigation. The report shall contain the proposals about the necessary security measurements for the prevention of the personal data breach.

The Data Controller shall decide about the implementation of the measures.

If the Data Controller thinks that the personal data breach is likely to result in a high risk to the rights and freedom of natural persons, it shall communicate the personal data breach to the data subject without undue delay.

The Data Controller shall clearly describe the nature of the personal data breach in an understandable way including the followings:

- the name and contact details of the person providing more information;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Data Controller shall not inform the data subjects if:

- it has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- it has taken subsequent measures which ensure that the high risk to the rights and freedom of data subjects is no longer likely to materialise;
- the information requires disproportionate effort, i.e. the number of the data subjects is so high that it would be disproportionately burdensome for the Data Controller to provide them with the above information. In this case, the Data Controller shall take measures about the disclosure of the appropriate information.

12. REGISTRATION OF THE PERSONAL DATA BREACH

The Data Controller shall keep records of the personal data breach.
The records shall include the below information:

- the categories of personal data concerned,
- the scope and number of data subjects concerned by the personal data breach,
- the date and time of the personal data breach,
- the circumstances and effects of the personal data breach,
- the measures taken to prevent the personal data breach,
- other data determined by the law prescribing the data processing.

The Data Controller shall keep the data regarding the personal data breaches in the records for 5 years in the case of incidents concerning personal data and for 20 years concerning incidents of special data.

13. THE RIGHT TO REMEDY

The Data Controller may be contacted via the contact details set out in this Policy in the case of any questions and comments concerning the data processing.
You can also lodge a complaint to or request remedies from the Hungarian National Authority for Data Protection and Freedom of Information:

Name: Hungarian National Authority for Data Protection and Freedom of Information
Registered office: H- 1055 Budapest, Falk Miksa utca 9-11.
Correspondence address: 1363 Budapest, Pf. 9.
Phone: +36-1-391-1400
Fax: +36-1-391-1410
Website: **www.naih.hu**
E-mail: **ugyfelszolgalat@naih.hu**

In the case of the breach of his/her rights, the data subject may go to the court against the Data Controller. The court shall act out of turn in the case. The Data Controller shall prove that the data processing complies with the provisions of law. The assessment of the litigation falls in the competence of the regional court. At the plaintiff's, i.e. the data subject's discretion, the litigation may be initiated at the regional court competent at the place of residence or location of the data subject.

The Data Controller hereby undertakes to cooperate with the competent court or the NAIH and provides the competent court or the NAIH with the data related to the processing.

The Data Controller also undertakes to compensate the data subject for the damage caused by the unlawful processing of the personal data or breaching the requirements of data security. The data subject

is entitled for a grievance award in the case of the breach of his/her personal rights. The Data Controller shall be exempted from the liability if the damage has been caused by any unavoidable reasons beyond the scope of the data processing, or if the impairment caused by the damage or the breach of the personal rights arose from the deliberate or grossly negligent behaviour of the data subject.

The Data Controller reserves the right to amend this Policy at any time.

Budapest, 17th April 2023