DATA PROCESSING AGREEMENT

This data processing agreement is entered into by and between:

A. The **Institution**,

hereinafter referred to as the “controller”,

B. **Dodona Learning Technologies BV**, registered under company number 1024.211.716, with its registered office at Ottergemsesteenweg-Zuid 808, box B226, 9000 Ghent, legally represented by MARA Consulting BV (with Matthias De Witte as its permanent representative), Director,

hereinafter referred to as the “**processor**”, and together with the controller hereinafter jointly referred to as the “**parties**”, and each separately as a “**party**”.

Article 1. Subject matter of the data processing agreement

1. The parties have entered into a main agreement whereby the processor provides a software solution for programming education to the controller. This main agreement results in the processor processing personal data on behalf of the controller.
2. In accordance with the GDPR[1], the parties set out in this data processing agreement their mutual rights and obligations for the processing of personal data that takes place in the context of the performance of the main agreement.
3. This data processing agreement includes three (3) appendices that form an integral part of this data processing agreement:
    a. Appendix 1, the privacy notice, includes the following elements:
        i. Subject, nature, and purpose of the processing(s);
        ii. Duration of the processing(s);
        iii. Categories of personal data being processed;
        iv. Categories of data subjects whose personal data are processed.
    b. Appendix 2 is the security appendix in which the processor describes the technical and organizational measures it takes to secure and protect personal data.
    c. Appendix 3 is the data breach notification form.
4. The processor shall provide these appendices prior to the conclusion of the data processing agreement and shall ensure that the controller is adequately informed in understandable language about the service(s) provided by the processor. The information enables the controller to understand which processing operations are inextricably linked to the service offered and for which optional processing operations the controller can make a choice.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 2. Division of roles

1. When processing personal data, the parties shall act in accordance with the applicable laws and regulations.
2. The processor shall provide the controller with all information necessary to enable proper compliance with the relevant privacy laws and regulations (including the GDPR).
3. The processor shall assist the controller in complying with all legal obligations regarding data protection.

Article 3. Use of personal data

1. The processor undertakes to use the personal data obtained from the controller only for the purpose and in the manner for which the controller has provided the data. The processor is therefore not permitted to carry out any data processing other than that for which the controller has given written instructions (on paper or electronically). This obligation applies both during the term of this agreement and after its expiry.
2. If, on the basis of a legal obligation or a court ruling against which no further appeal is possible, the processor must process the personal data outside the instructions of the controller, the processor shall inform the controller of this before commencing such processing.
3. If the processor uses the personal data outside the instructions of the controller, it shall itself become the controller for this processing.
4. If the processor believes that data processing is in violation of the GDPR, it shall immediately inform the controller thereof.

Article 4. Confidentiality

1. The processor guarantees that everyone, including its employees, representatives, and/or sub-processors, whom it involves in the processing of personal data, will treat this data as confidential and comply with the obligation of secrecy, both during and after the term of the main agreement.
2. The processor guarantees that anyone it authorizes to process personal data has contractually committed to maintaining confidentiality or is bound by an appropriate legal obligation of confidentiality.
3. The processor shall ensure that employees working under its authority have access to personal data only to the extent necessary for the performance of their duties.

Article 5. Security and control

1. The processor guarantees that it has taken appropriate technical and organizational measures to protect the personal data against loss or any form of unlawful processing. These measures ensure a level of protection appropriate to the state of the art, the costs of the measures, and the risks and nature of the processing.
2. The measures referred to in Article 5.1 shall in any case include:
    a. an appropriate information security policy;

b. measures to ensure that only authorized personnel have access to the personal data processed under the data processing agreement;

c. measures to protect personal data against accidental/unintentional or unlawful destruction, loss, accidental alteration, unauthorized or unlawful storage, access, blocking, or disclosure;

d. regular evaluation of the information security policy in order to supplement this policy in line with the latest state of the art, to tighten it up or to make improvements to the systems used in the context of the performance of the main agreement.

3. Appendix 2 provides, among other things, a general overview of the technical and organizational security measures taken by the processor. The processor shall keep this list up to date. The processor shall not weaken the technical and organizational measures taken or lower the level of security during the term of this data processing agreement without the prior consent of the controller.
4. The processor shall provide the controller with all information demonstrating that it complies with its security obligations. In addition to reports by the processor, this may be based on, but is not limited to, valid certification or equivalent means of control or evidence.
5. In addition to the measures listed in the above paragraphs, the controller has the right, in consultation with the processor, to have the processor's security policy assessed by an independent auditor. This auditor will only provide the audit report to parties that have mutually agreed on how to deal with the results of the audit. The costs of the audit shall be borne by the controller, unless the audit reveals major deficiencies that can be attributed to the processor.

Article 6. Breaches relating to personal data/data leaks

1. The parties shall have an appropriate policy for dealing with security incidents, including personal data breaches. The parties shall keep a record of all incidents and the corrective measures they have taken to prevent such incidents. The processor shall grant the controller access to this record at the latter's request.
2. If the processor detects a personal data breach in the context of this agreement, it shall immediately notify the controller, at the latest within 24 hours of detection, in accordance with the procedure described in the security appendix.
3. The processor shall immediately inform the controller if there is a suspicion that the personal data breach poses a high risk to the rights and freedoms of natural persons.
4. If it is not possible to provide all the required information at the same time, the information may be provided in stages without unreasonable delay.
5. In the event of a breach, the processor shall provide the controller with all relevant information about the breach, including the nature of the breach, the categories of data subjects and personal data concerned and, approximately, the number of data subjects and personal data concerned, the likely consequences of the personal data breach, the measures proposed or taken by the processor to address the breach or mitigate its possible adverse effects.
6. The parties shall take all reasonably necessary measures as soon as possible to prevent or limit (further) violations or infringements, and more specifically (further) violations of the GDPR or other regulations concerning the processing of personal data. The processor shall include these new measures in Appendix 2 (security appendix) of this data processing agreement.

7. In the event of a breach, the controller shall comply with the legal obligation to report to the supervisory authority. The processor shall enable the controller to take appropriate follow-up steps (or have them taken). Depending on the nature of the incident, the processor shall assist and advise the controller in this regard.
8. The time and costs incurred by the processor in fulfilling this obligation shall be borne by the processor and cannot be charged to the controller.

Article 7. Procedure for data subjects' rights

1. A request from a data subject regarding access, correction, supplementation, deletion, or blocking of personal data will be forwarded by the processor within 24 hours to the controller, who will handle the request further.
2. The processor shall cooperate fully with the controller in order to comply with the obligations under the GDPR within the legal deadlines, in particular the rights of data subjects such as a request for access, correction, supplementation, deletion, or blocking of personal data.
3. The time and costs incurred by the processor in fulfilling this obligation shall be borne by the processor and cannot be charged to the controller.

Article 8. Assistance with data protection impact assessment

1. The processor shall assist the controller in carrying out a data protection impact assessment (“**DPIA**”) and any resulting mandatory prior consultation of the Data Protection Authority (“**DPA**”).
2. The processor shall provide the controller with the information about the DPIA that it has carried out itself prior to the conclusion of the main agreement.
3. The time and costs incurred by the processor in performing this obligation shall be borne by the processor and may not be charged to the controller.

Article 9. Assistance with complaints

1. The processor shall assist the controller in:
   a. complying with requests from the DPA or another government agency; or
   b. handling complaints from data subjects.
2. A request or investigation by the DPA regarding the processing of personal data shall, to the extent permitted by law, be forwarded by the processor within 24 hours to the controller responsible for handling the request.
3. The time and costs incurred by the processor in fulfilling this obligation shall be borne by the processor and cannot be charged to the controller.

Article 10. Processing outside the European Economic Area (“EEA”)

1. The parties shall ensure that the processing of personal data outside the EEA takes place in accordance with legal requirements and any obligations incumbent on the controller in this regard.

2. If data is processed outside the EEA, this shall be indicated in Appendix 1, including a list of the countries where the data is processed and the safeguards demonstrating how the conditions imposed by the GDPR for transfers outside the EEA are met.

Article 11. Engagement of sub-processors

1. By agreeing to this data processing agreement, the controller grants the processor permission to engage sub-processors, whose identities and location details are included in the Privacy Notice.
2. The Institution can register for change notifications to that list by emailing the processor at privacy@dodona.be. The processor will send an email to such registered Institutions at least seven days before adding or replacing a sub-processor. During this seven-day objection period, an Institution may object on reasonable, documented privacy or security grounds. The processor will work with the Institution to disable the functionality in question or, if that is not feasible, to provide an appropriate solution. To address urgent security, availability, or continuity issues, the processor may engage a sub-processor without prior notice. The processor shall then promptly inform registered Institutions; the same seven-day objection period shall apply from the moment of notification.
3. The processor is obliged to impose on every sub-processor, by means of an agreement or other legal act, at least the same data protection obligations as those imposed on the processor in this data processing agreement. This includes, among other things, the obligation not to further process the personal data other than as agreed in this data processing agreement, and the obligation to comply with the confidentiality obligations, reporting obligations, cooperation obligations, and security measures relating to the processing of personal data as laid down in this data processing agreement. At the request of the controller, the processor shall provide copies of (the relevant passages from) these data processing agreements.

Article 12. Retention periods and destruction of personal data

1. The processor shall not process the personal data for longer than the retention periods specified in Appendix 1.
2. The processor is obliged to destroy (or have destroyed) the personal data processed on behalf of the controller after the expiry of the retention period or upon termination of the main agreement, at all locations, unless the personal data must be retained for longer, for example in the context of legal obligations. In the event of further storage, the data will be transferred by the processor to the controller in a machine-readable format, with as little data loss as possible and with a view to continuity within the controller.
3. The processor shall confirm to the controller (in writing or electronically) upon request that the processed personal data has been destroyed.
4. The processor shall inform all sub-processors involved in the processing of the personal data of the termination of the data processing agreement and shall ensure that all sub-processors destroy the personal data (or have it destroyed).

Article 13. Liability and indemnification

1. Each controller involved in the processing is liable for damage caused by processing that infringes the GDPR. A processor shall only be liable for damage caused by the processing if the processing does not comply with the obligations of the GDPR specifically aimed at processors or if it has acted outside or contrary to the lawful instructions of the controller. The controller or processor may be exempted from this liability if it proves that it is in no way responsible for the damage-causing event.
2. Where a controller or processor has compensated the damage in full, that controller or processor may recover from other controllers or processors involved in the processing the part of the damage corresponding to their share of liability for the damage, in accordance with the conditions set out in §1.

Article 14. Conflict and amendment of the data processing agreement

1. In the event of any conflict between the provisions of this data processing agreement and the provisions of the main agreement, the provisions of this data processing agreement shall prevail.
2. In the event that any provision of this data processing agreement is contrary to the regulations and is therefore voidable, the other provisions of this data processing agreement shall remain in full force and effect. In that case, the parties shall consult with each other to replace this provision(s) with enforceable alternative provision(s) that comply with the regulations. The replacement shall be made with the consent of both parties.

Article 15. Applicable law and competent court

1. This data processing agreement is governed by Belgian law.
2. All disputes shall preferably be settled amicably. If an amicable agreement cannot be reached, the dispute in question shall be submitted exclusively to the courts and tribunals of the district of Ghent.

Article 16. Duration and termination

1. The term of this data processing agreement is equal to the term of the main agreement concluded between the parties, including any extensions thereof.
2. If the processor fails to fulfill the obligations under this data processing agreement correctly and fails to take appropriate measures within a period of up to two months, the controller may, without prejudice to other grounds for termination as provided for in the main agreement, immediately terminate the main agreement after the aforementioned period of two months and/or terminate the processing order.
3. The termination of this data processing agreement does not release the parties from their obligations arising from this data processing agreement which, by their nature, are deemed to continue even after termination.

Appendices

Appendix 1: Privacy Notice
Appendix 2: Security Appendix
Appendix 3: Data Breach Notification Form

APPENDIX 1: Privacy notice

The Institution is increasingly using digital applications in education, research, and services. The use and delivery of these products and services requires data that can be traced back to individuals (such as students and staff members of the Institution). The controller must make agreements with processors about the use of that personal data. This notice provides the Institution, as the controller, with information about the services provided by the processor and what personal data the processor processes in doing so. All in all, it addresses the questions of "who, where, why, and how the data of the persons concerned is processed."

The use of this Privacy Notice helps the Institution to better understand how the product and/or service works and what data is exchanged for this purpose. Based on this notice, a register of processing activities can be further completed and maintained.

A. General information

Name of product and/or service:	Dodona
Name of processor and location details:	Dodona Learning Technologies BV Ottergemsesteenweg-Zuid 808, box B226 9000 Ghent
Brief explanation of how the product and service work:	Dodona is an online platform for learning to program
Link to provider and/or product page:	https://www.dodona.be
Users of the product or service:	Students & faculty

B. General information regarding the processing

Subject of the processing:	The processing operations relate to the provision and support of the Dodona online learning platform, including the management of user accounts, the processing of submitted assignments, and the generation of feedback and reports for educational purposes.
Duration of the processing operation(s):	For the duration of the main agreement
Nature of the processing:	Provision of, and possibility to modify, data for the delivery of the product and services set out in the main agreement.

Description of the specific services provided and associated processing	Processing operations that form an integral part of the service offered (*) see table below for more information: ☒ Consultation of personal data ☒ Storage of personal data ☒ Forwarding personal data ☐ Updating or modifying personal data ☐ Testing software ☐ Any other (describe briefly)

(*) The controller hereby issues the following instructions for the processing of personal data (without prejudice to the instructions that arise directly from the provisions of the main agreement or the data processing agreement or that are reasonably required for the proper performance by the processor of its obligations):

- ☒ Accessing personal data
  Services provided by the processor whereby the controller's personal data may be viewed by employees or subcontractors of the processor, including but not limited to service desk services, (remote) monitoring services, system management services, technical application management, vulnerability scanning services, reporting services in governance, and software asset management services.

- ☒ Personal data storage
  Services provided by the processor whereby the controller's personal data is stored with appropriate security, technical, and organizational measures in a storage system provided by the processor, including but not limited to cloud storage services, cloud backup services, file services, directory services, managed file transfer, and log file processing.

- ☒ Forwarding personal data
  Services provided by the processor whereby the controller's personal data is sent from, to, or between applications on a platform managed by the processor, including but not limited to LAN services, Wide Area Network services, data center interconnectivity services, load balancing, SAN switch interconnects, and services provided over Voice over Internet Protocol (VoIP).

- ☐ Updating or modifying personal data
  Services provided by the processor whereby the controller's personal data can be modified both manually and automatically, such as in an automated job flow supported by a job scheduling system.

- ☐ Software testing
  Services provided by the processor whereby databases of the controller containing personal data (personal data that has not been anonymized) are used outside the production environment (in testing, acceptance, etc.) as part of the testing process of the controller's software application.

- ☐ Any other:

C. Purposes

Purpose:

☐ Student administration, including:

- creating a student database;
- organizing education;
- organizing exams, recording exam results;
- calculating, invoicing, and collecting amounts due (financial management);
- communicating with students (and parents);
- handling disputes;
- the exchange of personal data with third parties, including:
  - DHO 2.0 in the context of the performance of their (legal) duties;
  - Other controllers in the event of a transfer to another controller;
  - Parties involved in the provision of internships or work placements, insofar as necessary and legally permitted.

☐ Student guidance: Guiding students in their knowledge, performance, or skills, monitoring their progress, and guiding students in their study and career choices.

☐ Administration: processing necessary for the organization of education, including: drawing up timetables, communication, etc.

☒ Providing or making available teaching materials for teaching and learning, including:

- the storage of learning, test, and exam results;
- the return of learning and test results to the controller;
- assessing learning and test results in order to obtain learning materials and test materials tailored to the specific learning needs of a student (including adaptive teaching materials);
- analysis and interpretation of learning results;
- the ability to exchange learning and test results between digital educational resources.

☐ Personnel administration: all administration related to personnel management, including:

- recruitment and selection of personnel;
- payroll administration;
- personnel policy with a view to evaluation, training, and career planning.

☒ Receiving/being able to use digital educational resources in accordance with the agreements made between the controller and the processor, including:

- obtaining access to the digital educational resources offered (identification, authentication, and authorization);
- the security, control, and prevention of misuse and improper use, and the prevention of inconsistency and unreliability in the personal data processed using the digital educational resource;
- the continuity and proper functioning of the digital educational resource in accordance with the agreements made between the controller and the processor (carrying out maintenance, making backups, making improvements after errors or inaccuracies have been detected, and obtaining support, etc.).

☐ The ability of the controller to make fully anonymized personal data available for research and analysis purposes in order to improve the quality of education.

☐ The implementation or application of other laws and regulations.

☐ Carrying out marketing and PR assignments (e.g., in the context of events, links to social media, postal mailings, etc.).

D. Categories of personal data and retention periods

Description and list of categories of personal data used:

☒ Administrative data: e.g., login details

☐ Medical data

☐ Social data

☒ Data concerning knowledge, performance, skills

☐ Data concerning attendance

☐ Financial data

☐ Lifestyle habits

☐ …

Retention periods for personal data:

As long as required to perform the services under the main agreement.

E. Categories of data subjects

☐ Prospective students

☒ Students

☐ Alumni

☐ Staff/contact persons of processors

☐ Customers (insofar as they are natural persons)

☐ Research participants

☐ Participants in continuing education

☐ Users of (IT) infrastructure

☒ Staff and employees of the Institution

☐ Others: please specify:

F. Storage of personal data:

Location/country of storage and processing of personal data:	Microsoft Azure data center “sweden-central”

If the personal data is stored outside the EEA, this must be explicitly stated and the appropriate safeguards (or a reference to them) must be included.

G. Subprocessors

The processor uses the following sub-processors for the service/product: see the overview at https://www.dodona.be/subprocessors.

H. Contact details

If you have any questions or comments about this document or the operation of this product or service, please contact: privacy@dodona.be.

APPENDIX 2: Security Appendix

In this appendix, the processor specifies the appropriate technical and organizational measures it takes to protect the personal data of the data subjects with regard to the following security aspects, including:

A. Measures to protect personal data against accidental or unlawful destruction, alteration, storage, access, or disclosure

- The processor has an appropriate policy for the security of the processing of personal data, which is periodically evaluated and, if necessary, adjusted.
- The processor takes measures to ensure that only authorized employees can access the processing of personal data within the framework of the data processing agreement via an authorization system. Under this system, employees do not have access to more data than is strictly necessary for their job.
- The processor has an information security coordinator to identify risks relating to the processing of personal data, promote security awareness, monitor facilities, and take measures to ensure compliance with the information security policy.
- Information security incidents are documented and used to optimize the information security policy.
- The processor has established a process for communicating about information security incidents.
- The processor enters into confidentiality agreements with employees and makes information security agreements.
- The processor promotes awareness, education, and training with regard to information security.

B. Measures to secure personal data and ensure the continuity of resources, the network, the server, and the application

Below is the report on the BIV classification, the degree of compliance, and an explanation of any deviations from the standards. In principle, the processor uses the 'ROSA Information Security and Privacy Certification Scheme' (available at www.edustandaard.nl) as an assessment framework and to create a solid baseline level of information security and privacy.

Assessment form	Self-assessment
Assessment performer	Bart Mesuere, CTO
Login page	https://dodona.be/nl/sign_in/
BIV classification	Availability: M, Integrity: M, Confidentiality: M

Category	**Measures**	**Compliance**	**Explanation**
		[Compliant/ Not compliant/Alternative measure]	[If "Not met," indicate how/when this will be corrected. If "Alternative measure," describe it.]
Availability	Design	Compliant	
	Capacity management	Compliant	
	Maintenance	Compliant	
	Testing	Compliant	
	Monitoring	Compliant	
	Recovery	Compliant	
Integrity	Traceability (users)	Compliant	
	Backup	Compliant	
	Application controls	Compliant	
	Non-repudiation (data)	Compliant	
	Traceability (technical management)	Compliant	
	Integrity control	Compliant	
	Non-repudiation (application)	Compliant	
Confidentiality	Data lifecycle	Compliant	
	Logical access	Compliant	
	Physical access	Compliant	
	Network access	Compliant	
	Separation of environments	Compliant	
	Transport and physical storage	Compliant	
	Logging	Compliant	
	Dealing with vulnerabilities	Compliant	

APPENDIX 3: Data breach notification form

Address details of your contact person at the Institution for the main agreement
Name
Position:
Telephone/mobile:
Email address:
Your address details
Name:
Position:
Phone/mobile:
Email address:
Date on which you, as the processor, complete this notification form:
Information about your organization (processor)
Company name (processor):
Address:
Postal code:
VAT number:
Description of the security incident
Who discovered the security incident?
Name:
Job title:
When was the security incident discovered:
Date:
Time:

Provide a brief summary of the security incident:
Indicate why the incident constitutes a data breach, a breach of personal data security, and when this became apparent:
When did the breach occur?
a. **On: [date and time]**
b. **Between: [date and time] and [date and time]**
c. **Not yet determined.**
d. **Anonymous report by a third party on ... [date]**
Personal data involved in the breach (circle as applicable):
- **None, the data cannot be traced back to an individual**
- **Name, address, place of residence**
- **Telephone numbers**
- **Email addresses**
- **Usernames, passwords, or other login details, customer numbers**
- **Financial data: account numbers, credit card numbers**
- **National registration number**
- **Copies of identity documents**
- **Gender, date of birth, and/or age**
- **Data about a person's race, origin, ethnicity, religion, belief, political opinion, trade union membership, sexual orientation**
- **Health data, biometric data with identical identification (fingerprint, finger scan, etc.) and/or genetic data (DNA test results)**
- **Criminal personal data or personal data about unlawful or disruptive behavior in connection with a prohibition imposed as a result of that behavior**
- **Data about a person's financial or economic situation, data about debts, salary and payment data**
- **Derived financial data (income category, home ownership, car ownership)**
- **Lifestyle characteristics (including family composition, living situation, interests, demographic characteristics (age, gender, nationality, occupation, education)**
- **Data obtained from (public) social profiles (Facebook, LinkedIn, and Twitter accounts, etc.)**

- **Audio recordings and/or visual material (photos, videos, etc.)**
- **Other, namely:**
Extent of the breach: how much personal data is involved?
How many individuals' personal data is involved in the breach?
a. **None, the data cannot be traced back to an individual**
b. **Not yet determined**
c. **At least …………………………………… (number), but no more than …………………………..(number) individuals involved**
Describe the group/category of people whose personal data is involved in the breach and indicate whether there are vulnerable individuals (children, people with health problems, elderly people, etc.) among them.
What are the consequences for these people? Are they at high risk of harm? What harm?
Type of data breach (circle what applies):
a. **Read-only (an unauthorized third party has been able to view (confidential) data. The processor still has the data in its possession.) - confidentiality is at risk**
b. **Copying (an unauthorized/unauthorized person has been able to copy data. The data is still in the possession of the processor.) - confidentiality is at risk**
c. **Modification (an unauthorized/unqualified party has been able to modify data in the processor's systems - integrity is compromised**
d. **Deletion or destruction (an unauthorized third party has deleted data from the processor's systems or destroyed data.) - Availability is compromised**
e. **Theft of data - Availability is compromised**
f. **Not yet known**
Encryption and hashing by unauthorized third parties
Has the personal data been rendered incomprehensible or inaccessible by unauthorized third parties, for example through encryption and hashing?
No
Yes
Partially, namely
If so, how has the personal data been encrypted:

Transfer – international
Does the breach relate to individuals from other EU countries or non-EU countries? - **No** - **Yes** - **If so, which EU countries or non-EU countries**
Has the personal data been transferred to non-EU countries? - **No** - **Yes** - **If so, which EU countries or non-EU countries**
Remedial security measures:
What security measures (technical and organizational) have been taken to address the breach and prevent further breaches?
Additional information
Who in your organization has more information about the breach?
Name of the processor's contact person:
Position:
Phone/mobile
Email address: