Hogeschooltaal

DATA PROCESSING AGREEMENT

16 JANUARY 2025

VERSION 2.0

THE UNDERSIGNED:

[**Name of Educational Institution**], with its registered office at [**Address**] in [**Town/City]**, Chamber of Commerce number [**CoC No**.] and legally represented by [**Representative**] (hereinafter referred to as: "the Controller");

and

DigiTaalbedrijf B.V. (brand name Hogeschooltaal) located at Reykjavikstraat 1, Helix Building, 3543 KH, Chamber of Commerce number 20138522 and legally represented by Anneke Blok (hereinafter: "**Processor**");

Hereinafter collectively referred to as: "**Parties**" and individually as the "**Party**";

PLEASE TAKE THE FOLLOWING INTO CONSIDERATION:

- On [**Insert Date**] the Parties concluded an agreement with reference [**Agreement Reference**] concerning [**Subject of The Agreement**]. For the purpose of the performance of the Agreement, the Processor processes Personal Data on behalf of the Controller;
- In the context of the performance of the Agreement, **DigiTaalbedrijf B.V. (brand name Hogeschooltaal)** is to be regarded as a Processor within the meaning of the GDPR and [**Name of Educational Institution**] can be regarded as Controller within the meaning of the GDPR;
- The Parties wish to handle the Personal Data that is or will be processed in performance of the Agreement with care and in accordance with the GDPR and other Applicable laws and regulations regarding the Processing of Personal Data;
- In accordance with the GDPR and other Applicable laws and regulations regarding the Processing of Personal Data, the Parties wish to record their rights and obligations with regard to the Processing of Personal Data of Data Subjects in Writing in this Processing Agreement.

AND HAVE AGREED AS FOLLOWS:

ARTICLE 1. DEFINITIONS

In this Processing Agreement, capitalized terms have the meaning given in this article. Where the definition in this article is included in the singular, it also includes the plural and vice versa, unless expressly stated otherwise or the context indicates otherwise. If a term written with a capital letter is not included in this Article, this term will be given the meaning of the definition set out in Article 4 of the GDPR.

1.1. **Agreement:** the agreement concluded between the Controller and the Processor and on the basis of which the Processor processes Personal Data for the Controller for the implementation of this agreement.

1.2. **Appendix:** an appendix to this Processing Agreement, which forms an integral part of this Processing Agreement.

1.3. **Applicable laws and regulations regarding the Processing of Personal Data:** the applicable laws and regulations and/or (further) treaties, regulations, directives, decisions, policies, instructions and/or recommendations of a competent government authority regarding the Processing of Personal Data, also including future amendments and/or supplements thereto, including Member State law implementing laws of the GDPR and the Telecommunications Act .

1.4. **Data Subject:** the identified or identifiable natural person to whom the Personal Data relates, as referred to in Article 4(1) GDPR.

1.5. **Education Service:** services provided by DigiTaalbedrijf which can be used to provide education. This includes teaching, coaching, training, learning, practicing and testing in the field of language proficiency and arithmetic, including the Instruction section, the Test section and educational services and supplies that are closely related

1.6. **Employee:** the employees engaged by the Processor and other persons, not being a Sub-processor, whose activities falls under its responsibility and who are engaged by the Processor to implement the Agreement. For the purposes of this Processing Agreement, the term employee includes, interim or temporary staff provided via (for example) an employment agency; Zelfstandigen Zonder Personeel (ZZP) working under the instructions of the Processor.

1.7. **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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).

1.8. **In Writing or Written:** in writing or electronically, as referred to in Article 6:227a of the Civil Code.

1.9. **DPIA:** the data protection impact assessment that is carried out before the Processing with regard to the effect of the intended processing activities on the protection of Personal Data, as referred to in Article 35 GDPR.

1.10. **Processing Agreement:** the present agreement including Appendices, as referred to in Article 28 paragraph 3 GDPR.

1.11. **Privacy Policy:** means the policy of the Processor which is available on https://www.hogeschooltaal.nl/privacy.

1.12. **Service:** the service or services to be provided by the Processor to the Controller under the Agreement.

1.13. **Special categories of Personal Data:** Personal data as referred to in Article 9 GDPR.

1.14. **Sub-processor:** another processor, including but not limited to group companies, sister companies, subsidiaries and auxiliary suppliers, engaged by the Processor to support the performance of the Agreement.

1.15. **Supervisory Authority:** one or more independent public authorities responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to the Processing of their Personal Data and to ensure the free movement of Personal Data within the Union, as referred to in Article 4(21) and Article 51 GDPR. In the Netherlands this is the Dutch Data Protection Authority.

ARTICLE 2. OBJECT OF THE PROCESSING AGREEMENT

2.1. The Processing Agreement forms an addition to the Agreement and supersedes any arrangements previously made between the Parties with regard to the Processing of Personal Data. In the event of any conflict between the provisions of the Processing Agreement and the Agreement, the provisions of the Processing Agreement shall prevail.

2.2. The provisions of the Processing Agreement apply to all Processing that takes place in the context of the performance of the Agreement.

2.3. The Controller assigns and instructs the Processor to process the Personal Data on behalf of the Controller.

2.3.1. The instructions of the Controller have been described in more detail in the Processing Agreement (including the Appendices) and the Agreement. The Controller may give reasonable additional or different instructions In Writing.

2.3.2. The Parties shall record in Appendix A which Processing operations the Processor carries out on the instructions of the Controller. The Processor is exclusively authorised to carry out the Processing specified in Appendix A.

2.4. The Processor and the Controller shall comply with the GDPR and other Applicable laws and regulations regarding the Processing of Personal Data. The Processor will immediately inform the Controller if, in the opinion of the Processor, an instruction from the Controller violates the GDPR and/or other Applicable laws and regulations regarding the Processing of Personal Data.

2.5. In the event the Processor determines the purpose and means of any part of the Processing of Personal Data, the Processor will be considered the Controller for those Processing Operations in accordance with the GDPR and Applicable laws and regulations regarding the Processing of Personal Data.

ARTICLE 3. PROVISION OF ASSISTANCE AND COOPERATION

3.1. The Processor shall provide the Controller with all necessary assistance and cooperation in ensuring that the Parties comply with the obligations under the GDPR and other Applicable laws and regulations regarding the Processing of Personal Data. To the extent that such assistance relates to the Processing of Personal Data for the purpose of the performance of the Agreement, the Processor shall in any event provide the Controller with such assistance relating to:

i. The security of Personal Data;

ii. Carrying out checks and audits;

iii. Carrying out DPIAs;

iv. Prior consultation with the Supervisory Authority;

v. Responding to requests from the Supervisory Authority or another government agency;

vi. Responding to requests from Data Subjects;

vii. Reporting Personal Data Breaches.

3.2. The provision of assistance and cooperation with regard to meeting the requests from Data Subjects will in any event include the following obligations on the part of the Processor:

i. Processor shall take all reasonable measures to ensure that the data subject can exercise his rights.

ii. If a Data Subject contacts the Processor directly with regard to exercising his rights, the Processor - unless explicitly instructed otherwise by the Controller - will not (substantively) respond to this, but will immediately inform the Controller and request further instructions.

iii. If the Processor offers the Service directly to the Data Subject, the Processor is obliged to inform the Data Subject on behalf of the Controller about the Processing of the

Personal Data of the Data Subject in a manner that is in accordance with the rights of the Data Subject.

3.3. The provision of assistance and cooperation with regard to meeting requests from the Supervisory Authority or another government body shall in any case constitute the following obligations for the Processor:

3.3.1. If the Processor receives a request or order from a Dutch and/or foreign government agency with regard to Personal Data, including but not limited to a request from the Supervisory Authority, the Processor will inform the Controller without delay, to the extent permitted by applicable laws for the Processor. When handling the request or order, the Processor shall observe all instructions from the Controller and the Processor shall provide the Controller with all reasonably necessary cooperation.

3.3.2. If the Processor is prohibited by law from fulfilling its obligations under Article 3.3.1 of this Processing Agreement, the Processor will represent the reasonable interests of the Controller. This in any case means:

i. The Processor will have a legal assessment carried out of the extent to which: (a) the Processor is legally obliged to comply with the request or order; and (b) the Processor is effectively prohibited from complying with its obligations in respect of the Controller under Article 3.3.1 this Processing Agreement.

ii. The Processor will only cooperate with the request or order if the Processor is legally obliged to do so and where possible, the Processor objects (in court) to the request or order or the prohibition to inform the Controller about this or to follow the instructions of the Controller.

iii. The Processor shall not provide more Personal Data than is strictly necessary to comply with the request or order.

iv. In the event of transfer within the meaning of Article 8 of this Processing Agreement, the Processor shall examine the possibilities of complying with Articles 44 up to and including 46 of the GDPR.

ARTICLE 4. ACCESS TO PERSONAL DATA

4.1. The Processor limits access to Personal Data to Employees, Sub-processors, Third Parties and other Recipients of Personal Data to a minimum necessary which is necessary for the performance of the Agreement.

4.2. The Controller grants general written authorisation to the Processor to engage Sub-processors for Processing of Personal Data in accordance with the GDPR and Applicable laws and regulations regarding the Processing of Personal Data. The list of Sub-Processors used by the Processor shall be made available on the Privacy Policy or can be accessed by clicking here.

4.3. The Processor shall inform the Controller in Writing about the changes to the Sub-Processors used by the Processor, by updating the Privacy Policy. The Controller can choose to opt-in to receive active notifications about changes to the list of sub-processors and Privacy Policy by clicking here.

4.4. The Controller may object to changes to the Sub-Processors used by the Processor, but this may not be done without important data protection reasons. Objection to the intended amendment to the Sub-Processors used by the Processor must be lodged In Writing to the Processor within fifteen days of notification of the change being made available on: support@digitaalbedrijf.nl.

4.5. In the event of an objection by the Controller, the Processor may, at his own discretion, render the service without the intended change of the Sub-Processor. In the event of an objection by the Controller, when the performance of the service is unreasonable for the Processor without the intended change to the Sub-Processor, the Parties may then enter into voluntary discussions to seek a resolution or the Parties can terminate the service in accordance with the Agreement.

4.6. The general written authorisation of the Controller to engage Sub-processors does not affect the obligations of the Processor arising from the Processing Agreement, including but not limited to Article 9 of this Processing Agreement.

4.7. The Processor imposes the similar relevant obligations included in the Processing Agreement on the (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors.

4.8. The Processor shall ensure that the persons authorised to process the Personal Data and other Recipients of Personal Data have undertaken to observe confidentiality or are bound by an appropriate legal obligation of confidentiality.

4.9. The Processor remains fully responsible and fully liable to the Controller for the fulfilment of the obligations by the (legal) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors, arising from the GDPR and/or other Applicable laws and regulations regarding the Processing of Personal Data and the obligations arising from the Agreement and the Processing Agreement.

ARTICLE 5. SECURITY

5.1. The Processor takes appropriate technical and organizational measures to ensure a level of security tailored to the risk, so that the Processing meets the requirements of the GDPR and other Applicable laws and regulations regarding the Processing of Personal Data and the protection of the rights of Data Subjects is guaranteed. To this end, the processor will at least take the technical and organizational measures included in Appendix B.

5.2. In assessing the appropriate level of security, the Processor shall take into account the state of the art, the cost of implementation, as well as the nature, scope, context and purposes of processing and the varying likelihood and severity of risks to the rights and freedoms of persons, particularly as a result of the destruction, loss, alteration, unauthorized disclosure of, or access to, data transmitted, stored or otherwise processed, whether accidental or unlawful.

5.3. The Processor records its security policy in Writing. At the request of the Controller, the Processor provides access to the Processor's security policy.

ARTICLE 6. AUDIT

6.1. The Processor is obliged to periodically have an independent expert conduct an audit of the Processor's organization, in order to demonstrate that the Processor complies with the provisions of the Agreement, the Processing Agreement, the GDPR and other Applicable laws and regulations regarding the Processing of Personal Data is sufficient. The costs of the periodic audit in Article 6.1 this Processing Agreement of will be borne by the Processor.

6.2. Subject to the terms of this Processing Agreement, the Processor carries out a periodic audit at least once every two years, as referred to in Article 6.1 this Processing Agreement.

6.2.1. If Special Categories of Personal Data are processed, the Processor will carry out a periodic audit at least once a year as referred to in Article 6.1 this Processing Agreement.

6.2.2. If the Processor only carries out processing operations that present a low risk to the rights and freedoms of the Data Subjects, the Processor shall not be obliged to carry out a periodic audit as referred to in Article 6.1 this Processing Agreement.

6.3. The Processor shall be obliged to make the findings of the independent expert from the periodic audit, on request In Writing, available to the Controller in the form of a statement, in which the expert:

6.3.1. Gives an opinion on the quality of the technical and organizational security measures implemented by the Processor in relation to the Processing performed by the Processor on behalf of the Controller.

6.3.2. Informs the Controller about other findings relevant for performance of this Processing Agreement, and compliance with the GDPR, and other Applicable laws and regulations concerning the Processing of Personal Data.

6.4. The Controller has the right, at his request, to have an audit carried out by a (legal) person authorized by the Controller, with regard to the Processing of the Personal Data by the Processor, in order to demonstrate that the Processor complies with the provisions of the Agreement, the Processing Agreement, the GDPR and other Applicable laws and regulations regarding the Processing of Personal Data.

6.5. In the event of an audit at the request of the Controller under Article 6.4 of this Processing Agreement, the costs of the audit and reasonable costs incurred by the Processor shall be fully borne by the Controller. The Controller shall notify the Processor in Writing at least thirty business days before the start of the audit. The audit must not unreasonably interfere with the normal business activities of the Processor.

6.6. If it is determined during the audit that the Processor has not complied with the provisions in the Agreement, the Processing Agreement, the GDPR and/or other Applicable laws and regulations regarding the Processing of Personal Data, the Processor will immediately take all reasonably necessary measures to ensure that the compliance of the Processor with these.

ARTICLE 7. PERSONAL DATA BREACH

7.1. The Processor shall inform the Controller of a Personal Data Breach without unreasonable delay and no later than 24 hours after becoming aware of such a Personal Data Breach. Processor informs Controller via the contact person and contact details of Controller as included in Appendix A and at least with regard to what is included in Appendix C. The processor warrants that the information provided to the best of the Processor's knowledge at that time, is complete, correct, and accurate.

7.2. If and to the extent that it is not possible for the Processor to provide all information relating to the aforesaid Personal Data Breach in Appendix C immediately, the information can be provided to the Controller in phases without undue further delay and in accordance with Article 7.1 of this Processing Agreement, the GDPR and Applicable laws and regulations regarding the Processing of Personal Data.

7.3. The Processor has adequate policies and procedures in place to ensure that it can:

i. Detect Personal Data Breaches at the earliest possible stage;

ii. Inform the Controller in accordance with Article 7.1 of this Processing Agreement;

iii. Respond adequately and promptly to any Personal Data Breach;

iv. Prevent unauthorized disclosure, alteration and provision or otherwise unlawful Processing and prevent its recurrence.

At the request of the Controller, the Processor shall provide information on, access to these policies and procedures drawn up by the Processor.

7.4. The Processor shall keep a Written register of all Personal Data Breaches that relate to or are related with the Agreement or its performance, including the facts concerning the Personal Data Breach, its consequences and the corrective measures taken. At the request of the Controller, the Processor will provide the Controller with relevant details from this register.

7.5. The Processor will refrain from reporting Personal Data Breaches to the Supervisory Authority and/or the affected Data Subjects, unless expressly requested to do so In Writing by the Controller or if required by the GDPR and Applicable laws and regulations regarding the Processing of Personal Data.

ARTICLE 8. TRANSFER OF PERSONAL DATA

8.1. The Controller hereby instructs the Processor that Personal Data may only be transferred by the Processor to countries outside the European Economic Area or international organizations if there is an adequate level of protection, Articles 44 to 49 of the GDPR and Applicable laws and regulations regarding the Processing of Personal Data are complied.

8.2. The Processor will inform the Controller in Writing of this transfer of Personal Data undertaken in accordance with Article 8.1 of this Processing Agreement, by updating the Privacy Policy (this information can be accessed by clicking here), unless that legislation prohibits this notification for important reasons of public interest. The Controller can choose to opt-in to receive active notifications about changes to the transfers and Privacy Policy by clicking here.

8.3. For clarity, the Processor is a company based in The Netherlands. However, in order for the performance of this Processing Agreement, some parts of the Processing by the Sub-Processors may result in the transfer of Personal Data in accordance with Article 8.1 of this Processing Agreement.

ARTICLE 9. CONFIDENTIALITY OF PERSONAL DATA

9.1. All Personal Data is classified as confidential data and shall be treated as such.

9.2. The Parties shall keep all Personal Data confidential and shall not further disclose it internally or externally in any way, except to the extent that:

i. Disclosure and/or provision of the Personal Data is necessary in the context of the performance of the Agreement or the Processing Agreement;

ii. Any mandatory Union or Member State law or a judicial decision of a competent court obliges the Parties to disclose, provide and/or transfer such Personal Data, whereby the Parties first inform the other Party thereof;

iii. Disclosure and/or provision of that Personal Data takes place with the prior Written consent of the other Party or the concerned end-users of the service.

9.3. The Parties are obliged to treat confidentially all knowledge of business secrets and data security measures of the other party, that were acquired within the scope of the contractual relationship, even beyond the termination of the. This also applies in particular to the contents of this Processing Agreement, as well as all documents, information made available within the framework of the audit. If there are any doubts as to whether information is subject to confidentiality, it shall be treated as confidential until it is released in writing by the other Party.

ARTICLE 10. LIABILITY AND INDEMNIFICATION

10.1. A Party cannot rely on a limitation of liability included in the Agreement or Processing Agreement or any other agreement or arrangement existing between the Parties with regard to any of the following instituted by the other Party:

i. action for recovery pursuant to Article 82 of the GDPR; or

ii. action for damages under the Data Processing Agreement, if and as far as the action consists of recovery of a fine paid to the supervisory authority that is fully or partially attributable to the other Party.

10.2. The provisions of this article shall not affect the legal remedies available to the aggrieved party under current laws or regulations.

10.3. Each Party is obliged to inform the other Party without undue delay of any (potential) notice of liability or the (potential) imposition of a fine by the supervisory authority, in both cases in connection with this Data Processing Agreement. Each Party is reasonably obliged to provide the other Party with information and/or support for advancing a defence against a (potential) notice of liability or fine, as referred to in the preceding sentence. The Party providing the information and/or support will have the right to charge reasonable costs incurred in this respect, if any, to the other Party. The Parties will inform each other of any such costs in advance as much as possible.

10.4. The Parties are each liable for their own damage arising from or related to failure to comply with the Processing Agreement and/or the GDPR and/or other Applicable laws and regulations regarding the Processing of Personal Data.

10.5. The Parties indemnify each other against damage or fines from Third Parties, including Data Subjects and the Supervisory Authority, which are caused by an attributable shortcoming of a Party and result in fines and/or damage against the other party due to a violation of the Processing Agreement and/or the GDPR.

ARTICLE 11. INCONSISTENCY AND AMENDMENT

11.1. In the event of any inconsistency between the provisions of this Processing Agreement and the provisions of the Agreement, the provisions of this Processing Agreement shall prevail.

11.2. The Processor is obliged to immediately inform the Controller in Writing of intended changes to the means of provision of the Service, the execution of the Agreement and the implementation of the Processing Agreement that relate to the Processing of Personal Data. This in any case means:

i. Changes that (may) affect the (categories of) Personal Data to be processed;

ii. Changes to the means by which the Personal Data are processed;

iii. Changes to Sub-processors used for the provision of services;

iv. Change in the transfer of Personal Data to third countries and/or international organizations;

v. Changes to the technical and organisational measures implemented by the Processor.

11.3. The Processor shall inform the Controller In Writing about the changes specified in Article 11.2 of this Processing Agreement, by updating the Privacy Policy. The Controller can choose to opt-in to receive active notifications about changes by clicking here.

11.4. The Controller may object to changes specified in Article 11.2 of this Processing Agreement In Writing to the Processor within fifteen days of notification of the change being made available on: support@digitaalbedrijf.nl. In the event of an objection by the Controller, the Processor may, at his own discretion, render the service without the intended change. In the event of an objection by the Controller, when the performance of the service is unreasonable for the Processor without the intended change, the Parties may then enter into voluntary discussions to seek a resolution, or the Parties can terminate the service in accordance with the Agreement.

11.5. In the event of any such substantial changes (which does not include the changes under Article 11.2 of this Processing Agreement) to the terms of this Processing Agreement, which result in the alteration of the service and/or inclusion of the additional services that affect the Processing of Personal Data, before OpCo accepts the relevant choice, OpCo will be informed in intelligible language of the consequences of these changes. "**Important changes**" will be understood to mean the following in any case: the addition or change of a functionality that leads to an enhancement with regard to the Personal Data to be Processed and the purposes for which the Personal Data are Processed. Any such substantial changes, which requires amendments to the terms of these articles of the Processing Agreement can only be agreed jointly in Writing.

11.6. Amendments to this Processing Agreement, including any assurances given by the Processor shall be made in Writing in accordance with the GDPR, which may be in an electronic format. The Parties agree that amendments to the Processing Agreement or new contracts shall be concluded in an electronic format in accordance with Article 28(9) GDPR.

11.7. Changes relating to the Processing of Personal Data may never result in the Controller being unable to comply with the GDPR and/or other Applicable laws and regulations regarding the Processing of Personal Data.

11.8. In the event that any provision of this Processing Agreement is or becomes null and void, voidable or otherwise unenforceable, the other provisions of this Processing Agreement will continue in full force and effect. In that case the Parties will consult with each other in order to replace the void, voidable or unenforceable provision with an enforceable alternative provision. In doing so, the Parties will take into account the purpose of and the meaning behind the void, voidable or unenforceable provision as much as possible.

ARTICLE 12. DURATION AND TERMINATION

12.1. The term of this Processing Agreement is equal to the term of the Agreement concluded between the Parties, including any renewals thereof.

12.2. This Processing Agreement will end by operation of law upon the termination of the Agreement. The termination of this Processing Agreement will not relieve the Parties of their obligations arising from this Processing Agreement (including obligations under Article 9 of this Processing Agreement) which, by their nature, are deemed to continue also after termination.

ARTICLE 13. MISCELLANEOUS PROVIONS

13.1. The Parties shall accept the conclusion of the contract in an electronic format in the sense of Article 28(9) of the GDPR.

13.2. This Processing Agreement shall form an integral part of the Agreement for the provision of services by the Processor to the Controller.

13.3. Within one month after the Agreement ends, the Processor will destroy and/or return all Personal Data and/or transfer it to the Controller and/or another party to be designated by the Controller, at the discretion of the Controller. All existing (other) copies of Personal Data, whether or not located with (legal) persons engaged by the Processor, including but not limited

to Employees and/or Sub-processors, are hereby demonstrably permanently deleted, unless done in accordance with the terms of this Processing Agreement or storage of the Personal Data is required by Union or Member State law is mandatory.

13.4. The Processor shall, at the request of the Controller, confirm in Writing that the Processor has fulfilled all obligations under Article 12.3 this Processing Agreement.

13.5. The Processor shall bear the reasonable costs for destruction, return and/or transfer of the Personal Data. The Controller may impose further requirements on the method of destruction, return and/or transfer of the Personal Data, including requirements on the file format. The transfer of Personal Data is based on an open file format. The Parties will agree in joint consultation on a reasonable distribution of any additional costs for the further requirements.

ARTICLE 14. GOVERNING LAW AND DISPUTE RESOLUTION

14.1. The Processing Agreement and its implementation are governed by Dutch law.

14.2. Disputes relating to the Agreement and this Processing Agreement are settled by the competent court in Utrecht, The Netherlands.

THUS AGREED BY THE PARTIES:

[Name of Controller]	DigiTaalbedrijf B.V.
_____/_____/_____ Date	_____/_____/_____ Date
_____ Name	Anneke Blok Name
_____ Signature	_____ Signature

Appendix A:

(Specification of the Processing of Personal Data)

Version number 2.0, Date of last modification: 16 January 2025

A. Description of the Processing
This Processing relates to the provision of the Education Service by DigiTaalbedrijf B.V. as described in the Agreement. This includes services provided by DigiTaalbedrijf B.V that can be used to provide education, for instance - teaching, coaching, training, learning, practicing and testing in the field of language proficiency and arithmetic, including the Instruction section, the Test section and educational services and supplies that are closely related

B. Purposes of the Processing
access and support for the digital learning platform part of the Education Service;
Storing, analysing, interpreting and assessing users' learning and test results;
return of learning and test results through the training;
assessment of learning and test results to obtain learning material and test material that is tailored to the specific learning needs of a student, thus making adaptive learning material and personalized learning paths;
assessment of the learning and test results of one student compared to the results of a standard group, to gain insight into how a student performs compared to this group;
receiving/being able to use the Education Service;
obtaining access to the Education Service, including identification, authentication and authorization;
security, control and prevention of abuse and improper use, and the prevention of inconsistency and unreliability in the processed personal data;
processing data for analytics by the Processor to provide insights in order to improve the quality of the Education Service, education and learning outcomes;
gathering, anonymizing and pseudonymising personal data for improving the quality of education and provide improved learning outcomes for the users;
providing customer support and receiving feedback from the users.

C. Categories of Data Subjects
Students
Teachers
Administrators of the Controller

D. Categories of Personal Data processed by the Processor

- Learning outcomes
- Access details
- Name of the student
- E-mail address
- Name of the teacher
- Name of the administrator of the Controller
- Student number
- School
- Surfconext ID
- LAS key or ECK
- Name
- Name of institution,
- Role (staff only)
- Year
- Group / class in educational institution
- Choice of class/group
- Device data including IP address
- Password
- Email address of teacher
- Practice assignments
- Test items
- Login activity of users
- Learning progress
- Test results
- Feedback from teacher of instructor
- Feedback from student
- Feedback from administrators
- Feedback from users of the Education Service
- Commonly used teaching materials
- Given answers and saved / stored results
- Customer tickets
- Customer feedback and surveys

E. Frequency of audit
Once every two years.

F. Retention period of the Personal Data
1 year after the license expires, all user data will be deleted (including test results and other results achieved) unless otherwise instructed by the Controller in writing via the contact details specified in the contract.

Categories Employees

Categories of Employees of Processor who Process Personal Data	Categories of Personal Data processed by Employees	Type of Processing	Country of Processing
Service & support employees of the Processor	• Name • Student number • Email • Education • Customer Feedback	• Customer support • Customer feedback	The Netherlands
IT management and platform services employees of the Processor	Categories of personal data specified in the Appendix A, Paragraph D of this agreement	• Provision of platform services • Maintenance and backup • Customer support • Improvement of platform and learning solutions	The Netherlands

Sub-processors

Sub-processor engaged by the Processor for the Processing of Personal Data	Categories of Personal data that Sub-processor processes	Type of Processing	Country of Processing
Infinitas Technology B.V.	• Learning outcomes • Access details • Name of the student • E-mail address • Name of the teacher • Name of the administrator of the Controller • Student number	• Providing access and support for the digital learning platform part of the Education Service; • Storing, analysing, interpreting and assessing users' learning and test results; • Return of learning and test results; • Assessment of learning and test results to obtain learning material and test material that is tailored to the specific learning needs of a student, thus making adaptive learning	The Netherlands

Sub-processor engaged by the Processor for the Processing of Personal Data	**Categories of Personal data that Sub-processor processes**	**Type of Processing**	**Country of Processing**
	• School • Surfconext ID • LAS key or ECK • Name • Name of institution, • Role (staff only) • Year • Group / class in educational institution • Choice of class/group • Device data including IP address • Password • Email address of teacher • Practice assignments • Test items • Login activity of users • Learning progress • Test results • Feedback from teacher of instructor • Feedback from student	material and personalized learning paths; • Assessment of the learning and test results of one student compared to the results of a standard group, to gain insight into how a student performs compared to this group; • Obtaining access to the Education Service, including identification, authentication and authorization • Securing, monitoring and preventing misuse and improper use of personal data • Gathering, anonymizing and pseudonymising personal data for improving the quality of education and provide improved learning outcomes for the users and quality of education. • Processing data for analytics by the Processor to provide insights in order to improve the quality of the Education Service, education and learning outcomes • Providing customer support and receiving feedback from the users • Processing feedback and user surveys	

Sub-processor engaged by the Processor for the Processing of Personal Data	Categories of Personal data that Sub-processor processes	Type of Processing	Country of Processing
	• Feedback from administrators • Feedback from users of the Education Service • Commonly used teaching materials • Given answers and saved / stored results • Customer tickets • Customer feedback and surveys		

Any relevant changes or latest details about sub-processors will be shared in the privacy policy on our website. Please see https://www.hogeschooltaal.nl/privacy

Transfers outside the European Economic Area

The Controller has given the Processor specific permission for the transfers to third countries or international organizations included below.

Description of transfer	Entity transferring the Personal Data and country	Entity receiving the Personal Data and country	Pass-through mechanism
Nil	Nil	Nil	Nil

Contact information

General contact details				
	Name	**Job title**	**E-mail address**	**Telephone number**
Controller	[Please provide the name of representative	[Please provide the job title of	[Please provide the email address of representative of the Customer]	[Please provide the telephone number of

General contact details				
	Name	**Job title**	**E-mail address**	**Telephone number**
	of the Customer]	representative of the Customer]		representative of the Customer]
Processor	Bob van Opstal	Segment manager Vocational & Higher Education	b.vanopstal@noordhoff.nl	+31505226748

Contact details in the event of a Personal Data Breach				
	Name	**Job title**	**E-mail address**	**Phone number**
Controller	[Please provide the name of the relevant person of the Customer]	[Please provide the job title of the relevant person of the Customer]	[Please provide the email address of the relevant person of the Customer]	[Please provide the telephone number of the relevant person of the Customer]
Processor	Maaike van Opstal	Data Protection Officer	privacy@infinitaslearning.com	+31 306383514
	Andrea Roagna	Security Officer	security@infinitaslearning.com	

Appendix B

(Security Measures)

Version number 2.0, Date of last modification: 16 January 2025

Details of the security measures taken by the Processor:
Only authorized personnel have access to the Processing of Personal Data
DigiTaalbedrijf uses an authorization policy to determine who should have access to which data. Under this system, employees do not have access to more data than is strictly necessary for their position.
Organization of information security and communication processes • DigiTaalbedrijf has established a privacy and security policy that describes the different roles. The following roles are important. • DigiTaalbedrijf has a data protection officer, who is primarily responsible for informing and advising DigiTaalbedrijf about its obligations under the GDPR and monitoring compliance. The responsibilities of this officer (DPO) are described in the appropriate Infinitas policy. Infinitas Learning is a group company. • The Corporate Security Officer (CSO) is responsible for Infinitas security policy. • Infinitas has appointed a local privacy contact per subsidiary and per jurisdiction ("Privacy Contact"), whose role is to implement and develop the entity's privacy policies and procedures for subsidiary management in collaboration with the DPO. • Information security incidents are documented and used to optimize the information security policy. • DigiTaalbedrijf has set up a process for dealing with (and communicating about) information security incidents (data breach procedure).
Staff • Confidentiality statements have been agreed with all employees in their employment conditions; • DigiTaalbedrijf encourages awareness, education and training regarding information security; • Based on an authorization system, employees do not have access to more data than is strictly necessary for their position. • Internal staff accounts are audited routinely using industry standard Microsoft tooling, this controls access to the Azure hosting environment. Direct access to the Databases containing data for DigiTaalbedrijf is controlled and managed by the engineering team working on the platform (Hogeschooltaal);
Technical Security Measures • Confidentiality obligation of employees and Third Parties involved, VoG obligation of security officer, awareness training for all employees. • Redundancy Hardware: hosts, storage and switches are redundant in the racks in the data center • Shielding Network: Double Firewalls and shielding network for many protocols

Details of the security measures taken by the Processor:

- Network Redundancy: Gigabit uplink in different racks in data center.
- Infinitas performs and tests incremental and full backups periodically on all critical business systems Monitoring:
  - All servers uplink, availability, storage space and load are monitored 24/7 by automatic systems such as Nagios and built in Azure monitoring.
  - Critical alerts are flagged to infrastructure team which is responsive during office hours (8 to 18) Monday to Friday.
- Fixed periodic updates on Linux and Windows servers.
- Active patch policy on shared servers.

DigiTaalbedrijf systems are periodically checked for security. In addition, DigiTaalbedrijf security policy provides internal processes to identify vulnerabilities. Informing about Data Leaks and/or security incidents

- The manner in which monitoring and identification of Data Leaks takes place

  DigiTaalbedrijf monitors its services 24/7 and has taken measures to prevent and identify unauthorized or unlawful access to data. Signals indicating a personal data breach are assessed by DigiTaalbedrijf Corporate Security Officer and Data Protection Officer, who analyzes whether there may be a personal data breach, the type of breach and whether this is a breach that falls under its role as processor or its role as controller.

- The way information is shared:

  If a personal data breach occurs with regard to personal data that DigiTaalbedrijf processes as a processor, the controller will be informed by or on behalf of DigiTaalbedrijf by e-mail within 24 hours after establishing that there has been a breach. Depending on the situation, information may also be shared via our website and official social media channels and/or official distributors and/or commercial agents.

- DigiTaalbedrijf shares the following information to data controllers when a personal data breach occurs:
  - The characteristics of the incident, such as: date and time of observation, incident summary, characteristic and nature of the incident (what part of security does it relate to, how did it occur, does it relate to reading, copying, changing, deleting/destroying) and/or theft of personal data);
  - The cause of the security incident;
  - The measures taken to prevent any/further damage; - Identifying those involved who may be affected by the incident, and to what extent;
  - The size of the group of people involved;
  - The type of data affected by the incident (in particular special data, or data of a sensitive nature, including access or identification data, financial data or learning achievements). If a specific situation lends itself to this, DigiTaalbedrijf can make a (first) report of a personal data breach to the authority. The controller will be informed about this and remains ultimately responsible for the report in this case.

Appendix C

(Information to be provided in the event of a Personal Data Breach)

Version number 2.0, Date of last modification: 16 January 2025

Details of the Personal Data Breach

1. Summary of the incident

2. How many people's Personal Data is involved in the Breach?

3. Describe the Categories of Data Subjects whose Personal Data is involved

4. When did the Breach occur?

- On (date) _____
- Between (period start date) and (period end date) _____
- Not yet known

5. What is the nature of the Infringement? (You can select multiple options)

- o Reading (confidentiality)
- o Copy
- o Change (integrity)
- o Removal or destruction (availability)
- o Theft
- o Not yet known

6. What type of Personal Data is involved? (You can select multiple options)

- o Name
- o Address
- o Telephone number
- o E-mail addresses or other addresses for electronic communications
- o Access or identification data (e.g. login name/password or customer number)
- o Date of birth
- o Age
- o Special categories of Personal

  _____
- o Other information, namely (complete)

  _____

  _____

  _____

  _____

7. What consequences could the Breach have for the personal privacy of the Data Subjects? (You can select multiple options)

- o Stigmatization or exclusion
- o Damage to health
- o Exposure to (identity) fraud
- o Exposure to spam or phishing
- o Other, namely (complete)

8. Follow-up actions following the Personal Data Breach

What technical and organizational measures has your organization taken to address the breach and prevent further breaches?

9. Technical protective measures

Is the Personal Data encrypted, hashed or otherwise made unintelligible or inaccessible to unauthorized persons? (Choose one of the following options and complete where necessary)

- ○ Yes
- ○ No
- ○ Partly, namely: (complete)

- ○ If the Personal Data has been made wholly or partly incomprehensible or inaccessible, how has this happened?

10. International aspects

Does the Infringement affect persons in other EU countries? (Choose one of the following options)

- ○ Yes
- ○ No
- ○ Not yet known