Televic Education

Personal data processing agreement

televic education

Version

Version	Issued by Process Owner + date	Reviewed by Process Owner(s) + date	Approved by Quality Mgt. + date	Valid from
1.01	EVL 07/05/2018	LC / GVD / JS 09/05/2018	LC / GVC / JS 09/05/2018	09/05/2018

Table of content

General info

This data processing agreement is an integral part of the Agreement between you (the other party) and Televic Education.

Televic Education is the processor (hereinafter: 'Processor') of the personal data and the other party is controller (hereinafter: 'Controller') of the personal data.

Whereas

1. The Controller collects and manages personal data in order to process and use them for the following objectives: testing and evaluating staff or educating and/or training students and/or staff.

2. The applicable Data Protection legislation (i.e. for example the General Data Protection Regulation and national data protection laws) requires the Controller to enter into a data processing agreement with the Processor.

3. The Controller wishes to process this personal data under the provisions mentioned below and entrust this to the Processor.

4. The Processor will process Personal Data (as further defined below) in the name of and on behalf of the Controller.

5. The Processor has declared and established credibly that he has the necessary competence and capacity to be able to properly perform this data processing and that he meets all legal requirements for this processing and can perform the processing while taking into account all statutory provisions.

6. The Parties have executed or shall execute this Data Processing Agreement (as further defined below).

Have agreed as follows

Articles

Article 1 – Definitions

Data Processing Agreement	means the present data processing agreement including its annexes;
Agreement	means the agreement between the Controller and the Processor;
Biometric Data	means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
Data Concerning Health	means Personal Data related to the physical or mental health of a natural person, including data concerning the provision of health care services, which reveal information about his or her health status, including a patient number, medical services, blood levels, etc.;
Data Subject(s)	means the identifiable or identified natural person(s) whose Personal Data is or are processed;
ECA	means the Act of 13 June 2005 concerning Electronic Communications;
General Data Protection Regulation or GDPR	means Regulation 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;
Genetic Data	means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Judicial Data	means Personal Data in related to judicial convictions, allegations and prosecutions regarding criminal offenses, proceedings pending before administrative authorities or courts, administrative sanctions and safety measures;
Personal Data	means any information which the Processor processes on behalf of the Controller within the framework of the Agreement and which can directly or indirectly identify the Data Subject;
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
Sensitive Data	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or revealing a trade union membership, as well as data regarding a person's sexual behavior or sexual orientation;
Special Categories of Personal Data	means one or more of the following categories of Personal Data: Data Concerning Health, Sensitive Data (including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning a natural person's sex life or sexual orientation), Genetic Data, Biometric Data or Judicial Data;

Article 2 – Object

2.1. The Processor shall exclusively and always process the Personal Data in the name and on behalf of the Controller. The Processor is not allowed to process the Personal Data in any form (not even in the form of anonymous or anonymized Personal Data) and in no way for his own account nor for the account of a third party. The Processor has no control on the purpose of the processing of Personal Data, nor may he independently take decisions concerning the use, storage or disclosure of the Personal Data, unless and to the extent it has been expressly agreed upon in the Data Processing Agreement, or instructed by the Controller, or when Processor has good faith that disclosure is reasonably necessary to comply with a law, regulation or compulsory legal request.

The Processor informs the Controller if he cannot comply with the instructions of the Controller or the obligations following this Data Processing Agreement, without undue delay and grants the right to the Controller to suspend the disclosure and transfer of Personal Data and/or to terminate this Data Processing Agreement in accordance with Article 10.3 of present Data Processing Agreement.

2.2. The Controller shall ensure that any disclosure of Personal Data to Processor is Personal Data that has been collected lawfully, i.e. processed on a legal basis as described in the articles 6-10 of the GDPR. The Controller shall indemnify Processor against all losses, expenses and liabilities incurred by Processor arising directly or indirectly from the Controller's breach of this obligation.

2.3. The subject, duration, nature and purpose of the processing, as well as the type of Personal Data being processed and the categories of Data Subjects, are listed in **Annex 1**. Any change in one of the elements listed in **Annex 1**, will result in an amendment of **Annex 1**, as mutually agreed by the Parties. If the Processor is aware of the fact that one of the elements listed in **Annex 1** will be changed, he must promptly inform the Controller hereof in writing.

2.4. The Processor only processes the Personal Data for the performance of its obligations under the Agreement, in accordance with the Data Processing Agreement and the written instructions of the Controller and shall perform the processing at all times with state of the art security measures and at all times in accordance with the minimum organisational and technical security measures as set out in **Annex 2** to this Data Processing Agreement. Any other use of the Personal Data by the Processor, in any form (even in the form of anonymous or anonymized Personal Data) or in any way, is not allowed. The Processor may not edit (nor have anyone edit) the Personal Data (such as but not limited to copying, printing, forwarding, enriching, modifying, etc.) unless and to the extent necessary for the performance of the Agreement and the Data Processing Agreement.

2.5. If the Processor processes one or more Special Categories of Personal Data in the name and on behalf of the Controller, it undertakes to comply with the additional specific obligations of **Annex 3**. In the event of any conflict or inconsistencies between the provisions of this Data Processing Agreement and **Annex 3**, the provisions of **Annex 3** shall prevail. If the Processor does not process Special Categories of Personal Data in the name of and on behalf of the Controller, then this Article and **Annex 3** are not applicable.

2.6. The Parties will, each in their respective capacity, process the Personal Data in accordance with the Data Protection Act, the ECA, the GDPR as of 25 May 2018, and any other applicable regulation to which the Controller and/or the Processor are subject.

2.7. The Processor acknowledges being granted or subject to the Processor-oriented rights and obligations under the Data Protection Act and, as of 25 May 2018, the GDPR. The Processor acknowledges that the Controller is granted or subject to the Controller-oriented rights and obligations under the Data Protection Act and, as of 25 May 2018, the GDPR.

2.8. The Processor commits to process the Personal Data in accordance with the content of **Annex 1**, in particular regarding the location of the processing.

Article 3 – Confidentiality

3.1. Regardless the type of Personal Data entrusted by Controller to Processor, the Processor shall treat the existence of the processing in name of and on behalf of the Controller, and the Personal Data, as strictly confidential. This duty of confidentiality is more stringent for the processing of Special Categories of Personal Data.

3.2. The Processor shall not disclose, in any form (including in the form of anonymous or anonymized Personal Data) or manner whatsoever, the Personal Data to third parties or grant third parties access to Personal Data, including to sub-processors, except in the cases and under the conditions provided for in Article 3.3.

The Processor shall exclusively and always process the personal data in the name and on behalf of the Client in order to perform this Agreement and in no way for his own account nor for the account of a third party.

3.3. The Processor may grant third parties access to the Personal Data in the event:

(i) the Controller gave its prior and explicit written approval – the Controller hereby agrees that access to the Personal Data is being granted to third parties listed in **Annex 1**. In the event the Controller agrees to grant such access to new third parties in the course of the Agreement, **Annex 1** shall be amended accordingly by mutual consent.

(ii) The Processor is required to grant such access under a mandatory Belgian or European provision of law. In this case unless such notification is prohibited by law or by overriding reasons of general interest, the Processor shall notify the Controller in advance and in writing about the request to access Personal Data, the relevant mandatory provision and the response the Processor intends to give to this request.

3.4. Except in the cases set out in Article 3.3 (ii), in the event the Processor grants third parties access to the Personal Data, it undertakes that each third party will be subject to contractual obligations at least equivalent to the ones to which the Processor is itself subject vis-à-vis the Controller under this Data Processing Agreement. The Processor guarantees that each third party, to whom it grants access to the Personal data, shall comply with these obligations.

3.5. The Processor can grant its employees access to the Personal Data in accordance with the need-to-know principle, i.e. to the extent the employees need such access to the Personal Data in order to allow a proper performance of the Processor's obligations under the Agreement and under the Data Processing Agreement. The Processor will inform the concerned employees in writing about the Personal Data's confidential character along with the Personal Data's legal and contractual framework, and shall impose a contractual confidentiality obligation upon the concerned employees. Processor shall impose a contractual confidentiality obligation upon the employees, that may have access to the Personal Data in order to perform the data processing, whose confidentiality obligation is identical to the present Article.

3.6. The Processor shall be responsible for complying with the duty of confidentiality by all people (i.e. employees and contractors) who are aware of the personal data and/or of its processing.

3.7. The Processor shall guarantee the confidentiality of the personal data to be processed and will take the necessary organizational and technical security measures as described in Annex 2 to this Data Processing agreement. These organizational and technical measures shall correspond to article 32 of the GDPR.

Article 4 – Obligation to assist

4.1. The Processor commits to assist the Controller in ensuring compliance with its legal obligations under the ECA (if applicable) and, as of 25 May 2018, the GDPR. In this regard the Processor shall respond within a reasonable delay to any request for assistance made by the Controller. In the event the Processor is of the opinion that a Controller's request or instruction infringes the ECA (if applicable) or, as of 25 May 2018, the GDPR, he will immediately notify the Controller. This assistance provided by the Processor to the Controller shall be subject to reasonable compensation.

4.2. Upon the Controller's request, the Processor shall inform the Controller about the modalities of its Personal Data's processing and shall grant access to the processed Personal Data and to all documents, buildings, systems, software, hardware, databases, installations and infrastructure necessary to enable the Controller to verify compliance with the ECA (if applicable) and, as of 25 May 2018, the GDPR.

4.3. Upon the Controller's request, the Processor shall accept and cooperate with audits and inspections of its Personal Data's processing so that the Controller is able to verify whether the Processor complies with its obligations following this Data Processing Agreement and the applicable data protection laws (GDPR and national data protection laws). The Controller may itself carry out these audits and inspections or mandate a third party thereto. If the Controller mandates a third party, such third party shall not be a direct competitor of Processor and such third party shall agree to be bound by confidentiality obligations that are no less protective than those set out in Article 3 of the Data Processing Agreement.

4.4. The Processor shall immediately transfer to the Controller any Data Subject's request or question in connection with the (processing of) Personal data. The Controller shall decide on the response to be given in that regard. On request of the Controller, the Processor shall assist and support the Controller in responding to such data subject's requests insofar reasonably possible for the Processor. In particular, the Processor shall, if and to the extent that it falls within its technical capabilities and powers under the Data Processing Agreement, comply within 5 working days with any Controller's request regarding the response or execution of the Data Subjects' requests. The Processor shall be entitled to reasonable compensation for this assistance.

4.5. To the extent that the Processor itself has communicated Personal Data to third parties, it shall without delay transfer to these third parties every Personal Data's alteration, erasure or restriction of which it becomes aware.

4.6. The Processor undertakes to assist the Controller in determining whether a data protection impact assessment is necessary for the Controller's processing of Personal Data. This implies for example that if the Processors' processing requires the use of new technologies, or if the Processor considers it plausible that the used technology may qualify as "new" and such new technology is likely to result in a high risk to the rights and freedoms of natural persons, the Processor notifies the Controller accordingly before starting the Personal Data's processing.

4.7. If the Controller is of the opinion that a data protection impact assessment must be conducted, the Processor commits itself to assist the Controller, upon its written request, in executing the data protection impact assessment. In such case the Processor provides the Controller with at least the information set out in Annex 3, and shall only begin the processing after receipt of the (evaluation of the) data protection impact assessment and the Controller's written instructions in that regard. The Processor shall be entitled to reasonable compensation for this assistance.

4.8. As of 25 May 2018, in the event a Data Subject wishes to exercise her/his right to data portability regarding Personal Data processed by the Processor in the name of and on behalf of the Controller, the Processor shall communicate the relevant Personal Data in a structured, standard and machine-readable form to the Controller or, at the request of the Controller, to the Data Subject. The Processor shall be entitled to reasonable compensation for this assistance.

Article 5 – Personal Data Breach

5.1. If a Personal Data Breach occurs or has occurred, the Processor shall, immediately after becoming aware of it, notify the Controller's legal department by telephone and by e-mail.

5.2. The Processor provides the Controller upon the notification of the incident, or if this is not feasible without undue delay after the notification of the Personal Data Breach, with the following information regarding the Personal Data Breach:

(i) the nature of the Personal Data Breach,
(ii) where possible the categories of Data Subject(s),
(iii) the estimated amount of Data Subject(s),
(iv) the categories of Personal Data,
(v) the estimated amount of Personal Data,
(vi) the name and contact details of the data protection officer if the Processor has appointed such an officer, or in the event that there is no data protection officer, another contact point where more information on the Personal Data Breach can be obtained,
(vii) the likely consequences and risks, including the likely consequences and risks for the Data Subjects,
(viii) the measures taken to address the Personal Data Breach, including, where appropriate, the measures to mitigate its possible adverse effects.

5.3. The Processor shall assist the Controller as much as possible when reporting a Personal Data Breach to the supervisory authority and/or the Data Subject(s). The Processor shall in any event respond on a priority basis to any question/request from the Controller regarding the Personal Data Breach.

Article 6 – Organisational and technical security measures

6.1. The Processor undertakes to implement and comply with the appropriate technical and organizational security measures necessary for the Personal Data's protection. The Processor will describe these measures in a security policy.

6.2. The Processor shall take into account the information provided by the Controller regarding the processing activities conducted on behalf of the Controller, when determining the appropriate technical and organizational security measures, (i) the state of the art, (ii) the implementation costs related to these measures, (iii) the nature, scope, context and purposes of processing, (iv) the risks involved for the Data Subjects' rights and freedoms, in particular in case of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or non-authorized access to Personal Data transmitted, stored or otherwise processed, and (v) the probability that the processing shall have an impact on the rights and freedoms of the Data Subjects. Without receiving sufficient and detailed information from the Controller, the Processor shall not be able to determine the necessary technical and organizational security measures.

6.3. The Processor shall update these measures on a regular basis according to the criteria referred to in Article 6.2 and by taking any incident into account.

6.4. The Processor shall implement the minimal appropriate technical and organizational security measures as listed in **Annex 2**.

Article 7 – Liability

7.1. The Processor is liable and shall indemnify the Controller for all principal sums, costs, interests and other expenses for the payment of damages caused to or claims from third parties, including the Data Subject, fines, administrative sanctions and other legal costs and other requirements by virtue of claims that may be filed against the Controller by individuals, by a data protection authority or by a government due to the Processor's breach of the Data Processing Agreement, the obligations specifically imposed on the Processor by the ECA (if applicable) and/or, as of 25 May 2018, the GDPR.

7.2. The Processor shall indemnify the Controller for all damages caused by third parties (i.e. sub-processors) appointed by the Processor.

7.3. The Controller must demonstrate the causal link between the damage suffered and the infringement of the Processor before being able to claim any compensation.

7.4. The Processor is only liable if the cause of the incident is the responsibility of the Processor. Consequential damage from an error at the Controller or another processor appointed by the Controller is excluded.

7.5. The total liability of the Processor will in any case not exceed the amount of the annual license with the Controller and can in any case not exceed the total insured amount, per policy period for all damages of all persons insured under all Insurance policies together: € 5.000.000.

7.6. The total liability of Processor shall, in any case, not exceed the total amount of charges paid by the Controller.

Article 8 – Force Majeure

8.1. The following force majeure circumstances apply if they occur after the execution of this Data Processing Agreement and which prevent its performance: labor disputes and all other circumstances, such as fire, mobilization, seizure, embargo, ban on currency transfer, revolt, a shortage of modes of transport, general scarcity of raw materials, limitations in energy use, if these other circumstances occur outside the will of the parties.

8.2. The party that appeals to the abovementioned circumstances must immediately inform the other party of the commencement as well as of the termination of the force majeure circumstances in writing.

The occurrence of one of these circumstances removes all liability of both the Controller and the Processor.

Article 9 – Transfer of Personal Data

9.1. The Processor cannot transfer Personal Data to a country outside the European Economic Area (i.e. at the moment the European Union, Liechtenstein, Iceland and Norway) unless that country or the undertaking(s) concerned (including companies linked to the Processor) to which the Personal Data are transferred guarantee(s) an adequate level of protection of Personal Data, and the Controller has given its prior written consent to the transfer. The Controller agrees to transfer the data to the countries listed in **Annex 1**.

9.2. A transfer to a country outside the European Economic Area is authorized without the Controller's written consent if this transfer is necessary on the basis of a rule of law which is mandatory under EU law or Belgian law. In such

case, the Processor shall notify the Controller in advance and in writing about the legal provision on the basis of which the Processor is obliged to transfer the Personal Data, unless the relevant legislation prohibits such notification for reasons of public interest.

9.3. The Processor guarantees that the country or the undertaking, to which the Personal Data are transferred, ensures an adequate level of protection of Personal Data.

9.4. In the event of a transfer of Personal Data by the Processor to a country outside the European Economic Area, the adequate level of protection is guaranteed by the signature of the European Commission Standard Contractual Clauses. The Parties acknowledge the lack of European Commission Standard Contractual Clauses for transfers "processor to sub-processor". This particular transfer can be regularized to the extent the Processor guarantees that the sub-processor will sign, at the Controller's discretion, the European Commission Standard Contractual Clauses "controller-processor" directly with the Controller or the European Commission Standard Clauses "controller-processor" with the Processor on behalf of the Controller. In both cases, the Processor shall indemnify the Controller for all damages and claims arising from the sub-processor's non-compliance with the European Commission Standard Contractual Clauses.

Article 10 – Duration and termination

10.1. The Data Processing Agreement shall enter into force on the date of its signature.

10.2. The Data Processing Agreement shall remain in force for the duration of the Agreement. This Data Processing Agreement shall terminate automatically if the Agreement terminates.

10.3. In case of a breach of one of the provisions of this Data Processing Agreement by a Party, it can be terminated immediately by the other Party at the expense of the Party that remains in default. Furthermore, this Data Processing Agreement can be terminated at any time with a two-month notice period, provided that the termination is communicated by registered letter.

10.4. Upon termination of the Data Processing Agreement, all Personal Data and any physical or electronic copies thereof must be immediately provided to the Controller in a structured, commonly used and (machine) readable format. The Processor shall, at the choice of the Controller, delete all Personal Data, at the end of the provision of services relating to data processing and deletes existing copies unless the storage of the Personal Data is required on the basis of EU law and/or Belgian law.

Article 11 – Applicable law & competent court

This Data Processing Agreement shall be exclusively governed by Belgian law.

All disputes arising from this Data Processing Agreement shall be settled exclusively by the Courts of Kortrijk.

Article 12 – Miscellaneous

12.1 The Data Processing Agreement is severable. If one or more provisions that do not affect the essence of the Data Processing Agreement are declared fully or partially invalid, void or unenforceable, this shall not affect the validity and enforceability of the remaining provisions of this Data Processing Agreement nor of the entire Agreement. The Data Processing Agreement will remain in force between the Parties, as if the invalid, void or unenforceable provision never existed.

12.2 In the aforementioned case, the Parties undertake to renegotiate in good faith the Data Processing Agreement in order to modify or replace the (fully or partially) void, invalid or unenforceable provision by a provision that most closely matches the purpose of the invalid, void or unenforceable provision.

12.3 The modifications of and supplements to the Data Processing Agreement are valid only if they are expressly agreed in writing between the Parties.

12.4 If a provision of the Agreement is incompatible or contradictory to the provisions of this Data Processing Agreement, the Data Processing Agreement will prevail.

12.5 If the Personal Data or the relationship between the Parties is subject to new (European) legislation or case law, the Parties agree to renegotiate in good faith the Data Processing Agreement, and to bring the Data Processing Agreement in line with the new (European) legislation or case law.

12.6 If the Processor is subject to a code of conduct or was certified with regard to the processing of Personal Data, it undertakes to comply with and to maintain this code of conduct or certification for the duration of the Data Processing Agreement.

*

* *

Drawn up in two original copies of which each party has declared to have received an original and signed copy at..... on .....

The Controller The Processor

Annexes

Annex 1 – Overview of the Agreement and the processing operations

A. Nature and purposes of the processing	testing and evaluating staff or educating and/or training students and/or staff
B. Type of Personal Data that are processed	identification data, training and education, movie captures, sound captures, profession and relations, answers to questions, translations
C. Types of Special Categories of Personal Data	None.
D. Categories of Data Subjects	students, teachers, staff, trainers
E. Location(s) of the processing of Personal Data	Belgium, The Netherlands
F. Third parties	No third party has access to the Personal Data, except for:
G. Third countries to which Personal Data are transferred	Personal Data will not be transferred to third countries, except for:

Annex 2 – Technical and organisational security measures

The Processor shall install and provide the following security measures in order to protect the personal data:

Organisational measures
- Acceptable use & Information Security Policy
- Raising staff's awareness through information and training
- Notification procedure in case of physical/technical incidents
- Disciplinary follow-up in case of non-compliance with one of the measures
Technical measures
- Back-up system
- Control of access (physically and logical)
- Authentication system
- Password policy
- User-ID policy
- Logging system, detection and analysis of the entrance
- Patching
- Anti-virus
- Fire wall
- Network security
- Surveillance, examination and maintenance of the systems

Annex 3 – Special Categories of Personal Data

In the event the Processor processes one or more categories of Special Personal Data on behalf of the Controller, it commits to comply with the following additional obligations. This **Annex 3** is not applicable if the Processor does not process Special Categories of Personal Data.

1. List of persons who have access to the Special Categories of Personal Data

The Processor will keep a list of the categories of persons having access to the Special Categories of Personal Data. The capacity of these (categories) of persons must also be included in the list.

This list must be made available to the Controller and the supervisory authority.

2. Data protection impact assessment

If the Processor is requested to process Special Categories of Personal Data on a large scale on behalf of the Controller, the Processor will not start the processing before a data protection impact assessment has been carried out by the Controller. In this case, the Processor will assist the Controller by providing the information set out in **Annex 4** to the Controller so that the Controller may conduct a Data Protection Impact Assessment.

3. Technical and organisational measures

Given the sensitivity of the Special Categories of Personal Data as listed in **Annex 1**, the Processor undertakes to implement the technical and organisational measures as defined and listed in **Annex 2**.

Annex 4 – Data protection impact assessment

In the event a data protection impact assessment must be carried out, the Processor assists the controller, where necessary and upon request. The Processor provides the following information to the Controller as soon as reasonably possible and insofar as the Controller has provided sufficient information to the Processor to conduct the assessment thoroughly and taking into account that the Processor processes the personal data on behalf of and under instruction of the Controller:

(i) A systematic description of the envisaged processing operations;
(ii) An assessment of the necessity and proportionality of the processing operations in relation to the purposes included in the Data Protection Agreement;
(iii) An assessment of the risks related to the Data Subjects' rights and freedoms;
(iv) The envisaged measures to address the risks, including safeguards, security measures and mechanisms intending to ensure the protection of Personal Data and to demonstrate compliance with the General Data Protection Regulation, taking into account the rights and legitimate interests of the Data Subject(s) and other concerned persons.