Model Data Processing Agreement Version 2.0

This is the English translation of the Dutch text of the Model Data Processing Agreement. In case the English translation differs or deviates from the Dutch text, the Dutch texts and interpretations prevail.

This Model Data Processing Agreement is an annex to the *Privacy Covenant Digital Educational Resources*(hereinafter referred to as the Covenant) concluded between the Primary Education Council (PO-Raad), Secondary Education Council (VO-Raad) and the branch organisations of educational publishing (GEU), distributors of learning resources (members of educational department of the Royal Book Seller Bond) and digital service providers in ICT education (VDOD).

The starting points of this Model Data Processing Agreement are in line with the provisions of the Covenant, the Personal Data Protection Act (hereinafter: Data Protection Act), and the starting points as indicated in case law and in guidelines and statements by the supervisory authority, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

The Model Data Processing Agreement version 2016 is the successor of the Model Data Processing Agreement which was drawn up in 2015 in the context of the Privacy Covenant *Digital Educational Resources, Learning resources and Testing*. In addition to using Learning Resources and Testing, the version 2.0 also covers School and Pupil Information Resources. In addition, some parts of the agreement have been adjusted in line with recent developments in legislation, including the amendment of the Data Protection Act in connection with the obligation to report Data Leaks.

The new Model Data Processing Agreement 2.0 replaces the Model Data Processing Agreement from 2015. Data Processing Agreements, already concluded based on the old model from 2015 remain in effect, in principle, until these Data Processing Agreement are terminated by the parties and are then followed by a new Data Processing Agreement based on the new Model Data Processing Agreement 2.0.

In the Covenant, it is agreed that Schools and Parties in the chain will use this model when making arrangements. If (parts of) the Model Data Processing Agreement cannot be used, only a substantiated written derogation is permitted. Given the number of provisions that are either required by law, or which the Dutch Data Protection Authority indicate that it must be included in the Data Processing Agreement, the scope for derogation from the provisions of the Model is limited.

This Model Data Processing Agreement contains two annexes:

1. The Privacy Leaflet (Annex 1) is a description of the service, product characteristics and which categories of Personal Data are processed and for which objectives these processing operations fall under.
2. The Technical and Organisational Measures (Annex 2) defines what security measures are taken. Security must remain a constant focus of attention and care.

Information about the Covenant and the Model Data Processing Agreement can be found on the website http://www.privacyconvenant.nl. More information and answers to questions about privacy and the legal rights and obligations for Schools can be found on

the websites of the industry councils Primary Education Council (PO-Raad) and Secondary Education Council (VO-raad) and Kennisnet.

June 2016

Parties:

1. The competent authority of <name + legal form of School>, registered under BRIN-number <brin> at the Dienst Uitvoering Onderwijs [Dutch Education Service] of the Ministry of Education, having its registered office and principal place of business at <address>, in (<postal code>) <city>, legally represented in this matter by <function + name>, hereinafter referred to as: '**School**".

and

2. The private limited company <Name> B.V., having its registered office and principal place of business at <address>, in (<postal code>) <city>, legally represented in this matter by <function + name>, hereinafter referred to as: '**Processor**"

Hereinafter collectively referred to as: '**Parties**', or separately: '**Party**"

Whereas:

a. School and Processor have concluded an agreement whereby <**specific description of products/services to be supplied by Processor on behalf of School**>, ('the Product and Services Agreement'). This Product and Services Agreement results in the Processor carrying out the processing of Personal Data on behalf of the School.
b. The parties wish, also in view of the provisions of Section 14 of the Personal Data Protection Act, to record their mutual rights and obligations for the Processing of Personal Data in this Data Processing Agreement.

agree to the following:

Clause 1: Definitions

In this Data Processing Agreement:

a. Data Subject, Processor, Third Party, Personal Data, Processing of Personal Data and Data Controller are understood according to the definitions defined in Section 1 of the Data Protection Act;
b. Data Processing Agreement: this Data Processing Agreement, including Annexes;
c. Annex: an annex to this Data Processing Agreement, which forms an integral part thereof;
d. Covenant: the *Privacy Covenant Digital Educational Resources;*
e. Data Leak: a security breach, as referred to in Section 13 Data Protection Act, which leads to the considerable risk of serious adverse effects, or serious adverse consequences for the protection of personal data, as referred to in Section 34a, subsection 1, Data Protection Act;
f. Digital Educational Resource: Learning Resources and Testing and School and Pupil Information Resources;
g. Learning Resources and Testing: digital product and/or digital service consisting of course material and/or tests and associated digital services, focussed on learning situations for the purpose of teaching by or on behalf of Schools;
h. School and Pupil Information Resources: a digital product and/or digital service for the benefit of the education (process), such as a pupil administration system, timetabling system, parent portal, pupil and parent communication system, an electronic learning environment and a pupil tracking system.
i. Privacy Leaflet: the privacy leaflet as set out in Annex 1;

j. Product and Services Agreement: the agreement between the School and Processor, as defined in paragraph a;
k. Model Data Processing Agreement The model for a data processing agreement as attached in the annex to the Covenant;
l. Sub-processor: the party that is engaged by the Processor as Processor for Processing of Personal Data in the context of this Data Processing Agreement and the Product and Services Agreement;
m. Data Protection Act: Wet bescherming persoonsgegevens [Dutch Personal Data Protection Act].

Clause 2: Subject and assignment of Data Processing Agreement

1. This Data Processing Agreement shall apply to the Processing of Personal Data in the context of the implementation of the Product and Services Agreement.
2. The School places with the Processor the contract for the Processing of Personal Data for the purpose of implementing the Product and Services Agreement.

Clause 3: Division of roles

1. The School is the Data Controller in respect of the Processing of Personal Data to be carried out on its behalf. The Processor is a processor within the meaning of the Data Protection Act. The School has and maintains independent control over the purpose and methods of the Processing of Personal Data.
2. The Processor shall ensure that the School, prior to the conclusion of this Data Processing Agreement, is sufficiently informed about the service(s) which the Processor provides, and the Processing to be carried out. The information given should enable the School to make a choice regarding the offered services as such, and in addition an individual choice for any optional services offered.
3. The services referred to in subclause 2, including any optional services, must be described in the Privacy Leaflet accompanying this Data Processing Agreement in plain language, whereby the School can give informed consent to the purchase of this service(s).
4. The School may be required to notify the Processing of Personal Data to the Dutch Data Protection Authority. The School shall examine whether or not it is exempt and shall notify the Dutch Data Protection Authority if it is obliged to do so.
5. The School and Processor shall provide each other back and forth, all the necessary information to allow proper compliance with the relevant privacy law and legislation.

Clause 4: Privacy Covenant

1. The Parties agree with the provisions in the Privacy Covenant Digital Educational Resources.

Clause 5: Use of Personal Data

1. Processor undertakes not to use the Personal Data received from the School for other purposes or in any other manner than for the objective, and the manner in which the data have been supplied or have become known. The Processor is therefore not allowed to carry out processing operations other than those assigned by the School (verbally, in writing or electronically) to the Processor. This obligation applies to both during the term of this agreement and after its completion.

2. An overview of the categories of Personal Data together with the use for which the Personal Data are processed are set out in the Privacy Leaflet annexed to this Data Processing Agreement.
3. The processor must indicate in the Privacy Leaflet whether or not the Privacy Leaflet relates to a Learning resource and Testing and/or School and Pupil Information Resource. The Processor must specify in the Privacy Leaflet for which purposes (included in the Covenant) Personal Data are processed when using his product and/or service and which categories of Personal Data are processed. If specified in the Explanatory Memorandum in the Privacy Leaflet, the Processor must also indicate under which of the objectives as defined in the Covenant, the Processing of Personal Data takes place when using the product and/or service.
4. The Processor refrains from transferring Personal Data to a Third Party, unless this exchange takes place on behalf of the School or when this is necessary in order to comply with a legal obligation imposed on the Processor. In the event of a legal obligation, prior to transferring, the Processor must verify the basis of the request and the identity of the applicant. In addition, the Processor will inform the School - if permitted by law - immediately, if possible prior to transferring.
5. *SPECIFIC PROVISION IN CASE OF EXCHANGING THE EDUCATIONAL REPORT: In addition to the provisions of subclause 4, it applies that, if the Processor is asked to transfer Personal Data to a Third Party designated and selected by the School, i.e. another School, the Processor will only proceed with transferring after the latter School has provided its administrative education identity (e.g. BRIN or OiN), insofar as it is known.*
6. *[SPECIFIC PROVISION IN CASE OF DISTRIBUTION OF LEARNING RESOURCES: Every year, when drawing up the learning resources lists for the next school year, whereby the learning resources lists are drawn up for the purpose of performing the Product and Services Agreement, the Parties will supplement and/or change the Privacy Leaflet by including the categories of Personal Data and the use of such Personal Data, with regard to the (digital) learning resources that are included on the relevant learning resources lists.]*

Clause 6: Confidentiality

1. The Processor ensures that everyone, including its employees, agents and/or Sub-processors, who are involved in the Processing of Personal Data, treat this data as confidential. The Processor ensures that each person who is involved in the Processing of Personal Data has entered into a confidentiality agreement or accepted a confidentiality clause.
2. The confidentiality obligation referred to in this Clause does not apply if the School has given explicit consent to disclose the Personal Data to a Third Party, if disclosure of Personal Data to a Third Party is necessary in view of the nature of services provided by the Processor to the School, or if there is a legal obligation to disclose the Personal Data to a Third Party.

Clause 7: Security and control

1. The Processor will, in the same way as the School, ensure appropriate technical and organisational measures to protect Personal Data against loss or any form of unlawful Processing. These measures, in accordance with the state of technology and the costs involved with the implementation and the execution of the measures, must ensure an adequate level of protection, taking account of the risks associated with the Processing of Personal Data and the nature thereof.

2. The measures specified in Clause 7.1 shall include at least:

a. measures to ensure that only authorised personnel have access to the Personal Data that is processed in the context of the Data Processing Agreement;

b. measures to protect the Personal Data against, in particular, accidental or unlawful destruction, loss, accidental alteration, unauthorised or unlawful storage, access or disclosure;

c. measures to identify weaknesses in respect of the Processing of Personal Data in the systems used for the provision of services to the School;

d. an appropriate information security policy for the Processing of Personal Data.

3. The Processor must evaluate, tighten up, supplement or improve the information security measures it has taken to the extent warranted by the requirements or (technological) developments.

4. Annex 2 establishes the arrangements between the Parties on the technical and organisational security measures, as well as on the content and frequency of the reports which the Processor provides to the School about the security measures. These measures are in line with the security measures that the School must take.

5. The Processor enables the School to meet its legal obligation to monitor compliance of the Processor of the technical and organisational security measures as well as on compliance with the obligations referred to in Article 8 in respect of Data Leaks. In addition to reports by the Processor, this can be achieved on the basis of, but not limited to, a valid certification or an equivalent verification or proof of evidence.

6. In addition to Clause 7 (4) the School has the right at all times, in consultation with the Processor and within a reasonable period of time, at its own cost, to have the technical and organisational security measures of the Processor audited by an independent Registered EDP auditor. The Parties, in mutual agreement, may agree that the audit is performed by a certified and independent auditor appointed by the Processor who will issue a third-party declaration (TPM). The School will be informed of the results of the audit.

Clause 8: Data Leaks

1. The Processor has an appropriate policy for dealing with Data Leaks.

2. If the School or Processor establishes a Data Leak, they will immediately inform the other Party. In the event of a Data Leak, the Processor shall provide all relevant information to the Data Controller with regard to the Data Leak, including information on any developments around the Data Leak, and the measures taken by the Processor to limit the effects of the Data Leak and to prevent recurrence. Additionally, the Parties will inform each other without delay if it transpires that the security breach is likely to have a negative impact on the privacy of the Party concerned as referred to in Section 34a, subsection 2, Data Protection Act.

3. In the event of a Data Leak, the Processor will enable the Data Controller to take the necessary follow-up steps with respect to the Data Leak. The Processor must follow the existing processes that the Data Controller has established for this purpose. The Parties will take as soon as possible all reasonably required measures to prevent or limit (further) breaches or infringements concerning the Processing of Personal Data, and more particularly (further) breaches of the Data Protection Act or other legislation concerning the Processing of Personal Data.

4. In the event of a Data Leak, the School must comply with any legal reporting obligation. The Parties may mutually determine whether and if so how, the Processor can make a notification to the Dutch Data Protection Authority. At the request of the School, the Processor can assist and advise the School with this. If required, the School will inform the Parties concerned about such an infringement. The Parties will, in good faith and in mutual consultation, make arrangements about the reasonable distribution of any costs associated with complying with the reporting obligations.
5. The Processor will inform the School in accordance with the arrangements laid down in Annex 2 on security related incidents, other than a Data Leak, which fall outside the scope of Clause 1 (e).

Clause 9: Procedural rights of Data Subjects

1. A complaint or request of a Data Subject with regard to the Processing of Personal Data will be forwarded immediately by the Processor to the School with responsibility for handling the request.
2. The Processor fully cooperates with the School - to the extent reasonably possible - to be able to meet the obligations under the Data Protection Act within the statutory deadlines, in particular, the rights of the Data Subjects, such as a request for access, correction, addition, removal or blocking of Personal Data. The parties will consult in good faith on the reasonable distribution of any costs involved in this.

Clause 10: Processing outside the European Economic Area

1. The Parties shall ensure that insofar as Personal Data are processed outside the European Economic Area (hereinafter referred to as: EEA), this takes place only in accordance with legislative requirements and any obligations resting on the Schools in this regard. If data are processed outside the EEA, this is specified in Annex 1, including an indication of the countries where the data will be processed.

Clause 11: Engaging Sub-processors

1. The Processor can engage a Sub-processor, whose identity and location information are to be included in the Privacy Leaflet.
2. The Processor requires each Sub-processor contractually to comply with confidentiality obligations, reporting obligations and security measures with regard to the Processing of Personal Data, which obligations and measures must al least comply with the provisions of this Data Processing Agreement.
3. The Processor requires each Sub-processor contractually not to process Personal Data in any other manner than agreed in this Data Processing Agreement.

Clause 12: Retention periods and destruction of Personal Data

1. The School will adequately inform the Processor about (legal) retention periods that apply to the Processing of Personal Data by the Processor. The Processor will not process the Personal Data for longer than these retention periods.
2. The School requires the Processor to destroy the Personal Data processed on behalf of the School, or have them destroyed, upon the termination of the Data Processing Agreement, unless the Personal Data should be kept for a longer period, such as in the context of legal obligations, or at the request of the School. The School may carry out an audit at its own expense whether destruction has taken place.

3. The Processor will give the School written or electronic confirmation that the destruction of the Processed Personal Data has taken place.
4. The Processor will inform all Sub-processors involved in the Processing of Personal Data of a termination of the Data Processing Agreement and will ensure that all Sub-processors will or have the Personal Data destroyed.

Clause 13: Contradiction and amending the Data Processing Agreement

1. In case of conflict between the provisions of this Data Processing Agreement and the provisions of the Product and Services Agreement, the provisions of this Data Processing Agreement will prevail.
2. If the Parties have to deviate from the articles in the Model Data Processing Agreement due to circumstances, or want to make additions, these changes and/or additions will be defined and substantiated by the Parties in an overview that is attached as Annex 3 to this Data Processing Agreement. The provisions of this paragraph shall not apply to additions and/or amendments of the Annexes 1 and 2.
3. In the event of significant changes to the product and/or the (additional) services that impact the Processing of Personal Data, the School will be informed in plain language about the implications of these changes before the School chooses to accept this. Important changes will mean in any case: adding or amending a functionality that leads to an increase in respect of the Personal Data to be processed, the objectives for which the Personal Data are processed and the engagement of a Sub-processor or different Sub-processor. The amendments will be incorporated in Annex 1.
4. Amendments to the Clauses of the Data Processing Agreement can only be effected by joint agreement.
5. In the event that any provision of this Data Processing Agreement is or becomes invalid, voidable or otherwise unenforceable, the remaining provisions of this Data Processing Agreement remain in full force and effect. In that case, the Parties will enter into consultation to replace the invalid, voidable or otherwise unenforceable provision by an enforceable alternative provision. The parties will take the utmost account of the purpose and intent of the invalid, void or otherwise unenforceable provision.

Clause 14: Duration and termination

1. The duration of this Data Processing Agreement is equal to the duration of the Product and Services Agreement concluded between the Parties, including any extensions thereof.
2. This Data Processing Agreement will end automatically upon termination of the Product and Services Agreement. The termination of this Data Processing Agreement will not exempt the Parties from their obligations arising from this Data Processing Agreement which by their nature are expected to continue after termination.

ANNEX 1: PRIVACY LEAFLET [name of product/service]

Schools are increasingly using digital applications within education. The use and provision of these products and services requires data that can be traced back to individuals (such as pupils). Schools must make arrangements with Processors on the use of such Personal Data. This leaflet gives schools information about the service the processor provides and what personal data the processor will process. In short, about the question "who, what, where, why and how" deals with the privacy of the persons concerned whose data are exchanged.

Using this Privacy Leaflet helps Schools to better understand the function of the product and/or service and what types of data are to be exchanged.

In the context of the recognisability, it is desirable that Processors use this Privacy Leaflet as much as possible in a uniform manner. Deviations from this model are indeed possible but should preferably be limited. If the space in this Annex is insufficient to describe the required information, is it possible to include the information in a separate annex or annexes, which shall be numbered as follows: "Annex 1A", "Annex 1B", etc. These Annexes will be attached to the Data Processing Agreement.

A. General information

Name of product and/or service :

Name of Processor and location information :

Brief explanation and functioning of product and service :

Link to supplier and/or product page :

Target group (such as PE/SE lower/upper) :

User : pupils/parents/guardians/teachers

B. The specific services

Description of the specific services provided and associated Processing

1. Processing which form an integral part of the service offered.

a. [….]
b. [….]

[….]

2. Description of the optional Processing offered by the processor

Explanation: This relates to additional services and associated Processing which do not form an integral part of the service offered. These include, for example, optional services for the School that may be helpful to the School for the purposes of the primary (learning) process and administrative work

The School must choose (order) the purchase of these services. This can be achieved by indicating this choice in writing in this Annex (for example, by ticking a tick box)☑). Agreement can also take place by means of the School activating the service in practice, for example, by switching a product or service on or off. The School that makes the choice in this way , must be able to do so on the basis of previously provided information (such as, for instance, listed in this leaflet).

a. [….]
b. [….]

[….]

C. Objectives for the processing of data

The Processor must explicitly indicate in this Leaflet whether it is:

- □ I. a supplier of a digital product and/or digital service consisting of course material and/or tests, or
- □ II. (also) a supplier of a School and Pupil Information Resources.

Re I. If the Processor is a supplier of a digital product and/or digital service consisting of Learning Resources and Testing, then the possible objectives of these products and services are defined in the relevant part of Clause 5 (1) of the Privacy Covenant Digital Educational Resources 2.0. These do not need to be further named in this Leaflet.

Re II. Only if the processor is (also) a supplier of a digital product and/or digital service consisting of a School and Pupil Information Resource, this Privacy Leaflet should explicitly mention the purposes for which Personal Data are processed when using the product and/or the service. The Processor must follow as closely as possible the list of objectives laid down in Clause 5 (2) of the Privacy Covenant Digital Educational Resources.

D. Categories and types of personal data

Description and summary of categories of Personal Data which are used:

Any optional Personal Data (which are not requested and stored as standard):

Types of data (such as special data or financial information):

E. General information on security measures taken:

For the sake of brevity, please refer to Annex 2 to the Data Processing Agreement for the security measures taken..

Specific security measures for this service/product [if applicable]:

Any certifications:

Audits/Third Party declarations:

City/Country of storage and Processing of Personal Data:

F. Sub-processors

The Processor engages the following Sub-processors for the service/product:

[party name, brief description of task/service showing what data are processed by this Sub-processor]

City/Country of storage and Processing of Personal Data (if the Personal Data are processed outside the EEA, a separate report must be made of the countries where the Personal Data are processed).

G. Contact details

For questions or comments about this leaflet or the operation of the product or service, please contact: [contact information].

H. Version [version number and date of last modification]

This privacy leaflet is part of the arrangements made in the Privacy Covenant Digital Educational Resources 2.0, an initiative of the Primary Education Council, Secondary Education Council, the various interested parties (GEU, KBB-e and VDOD) and the Ministry of Education, Culture and Science. You can find more information on: http://ww.privacyconvenant.nl.

ANNEX 2: Technical and organisational security measures

The Processor, in accordance with the Data Protection Act and Clause 7 of the Data Processing Agreement, is obliged to take technical and organisational measures to ensure the security of the Processing of Personal Data.

If the space in this Annex is insufficient to describe the required information, is it possible to include the information in a separate annex or annexes, which shall be numbered as follows: "Annex 2A", "Annex 2B", etc. These Annexes will be attached to the Data Processing Agreement.

Description of the measures as referred to in Clause 7.2 of the Data Processing Agreement.

I. Description of the measures taken to ensure that only authorised personnel have access to the Processing of Personal Data.

More specifically, an overview of which (groups of) employees of the Processor have access to which Personal Data, including a description of the operations these employees may carry out with the Personal Data.

a. (groups of) employees who have access to which Personal Data:

b. operations that these employees perform using the Personal Data:

II. Description of the measures to protect Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorised or unlawful storage, Processing, access or disclosure.

More specifically, an overview of the technical and organisational (security) measures taken by the Processor and the security standard used.

[description of security of the application/platform]

[description of method of identification/authentication/authorisation and security thereof]

[description of security of method of exchange/transport of data]

III. Description of the measures to identify weaknesses in respect of the Processing of Personal Data in the systems used for the provision of services to the School;

[such as a periodic analysis of (security) incidents, periodically conducting an external/ internal vulnerabilities investigation (ethical hack) or periodically conducting checks on the security of systems]

Reporting (Clause 7.4 of the Data Processing Agreement

The Processor reports periodically with a frequency of [...] times a year, by [...] to the Data Controller on the measures taken by the Processor on the technical and organisational security measures and any concerns therein.]

[contact details helpdesk/service desk for security incidents]

Informing about Data Leaks and/or security related incidents

Arrangements on the provision of information in the event of Data Leaks and/or security related incidents, in particular on

- The way in which monitoring and identification of incidents takes place,
- The way in which information is shared:
  - In what way (via e-mail, telephone);
  - To whom it should be addressed (contact person and contact details);
  - Whom should be contacted (for follow-up actions).
- Information that must be shared in any case about an incident
  - The characteristics of the incident such as: date and time of discovery, summary of the incident, attribute and type of incident (what part of security does it relate to, how has it occurred, does it relate to reading, copying, modifying, deleting/destructing and/or theft of personal data);
  - The cause of the security incident;
  - The measures taken to prevent any damage or further damage;
  - Naming Data Subjects who may be affected by the incident and the extent;
  - The size of the group of Data Subjects;
  - 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 performance).
- Any arrangements if, and if so how, the Processor can make a notification to the Dutch Data Protection Authority.

Version

[version number and date of the most recent amendment]

This privacy leaflet is part of the arrangements made in the Privacy Covenant Digital Educational Resources 2.0, an initiative of the Primary Education Council, Secondary Education Council, the various interested parties (GEU, KBB-e and VDOD) and the Ministry of Education, Culture and Science. You can find more information on: http://ww.privacyconvenant.nl.