Standard requirements for the Annexes to the Data Processing Agreement 4.0

This document is not intended to be completed by the Parties. It only sets out the requirements that the Annexes to the Model Data Processing Agreement must fulfil.

Requirements for Annex 1: the Privacy Annex

The Privacy Annex is an annex to the Model Data Processing Agreement and comprises the Instructions for the Processing of Personal Data from the Educational Institution to the Processor. It provides Educational Institutions with information on the services that the Educational Institution purchases from the Processor and records which Personal Data the Processor processes on the Educational Institution's behalf.

Parties to the Privacy Covenant affiliated with a sector organisation that is a joint Initiator of the Privacy Covenant (MEVW, VDOD, KBb-E) use the Privacy Annex that has been drawn up by this sector organisation, if available. The relevant sector model can be found on www.privacyconvenant.nl

The Privacy Annex for [name of product/service] must cover at least the following topics.

A. Contact details of the Processor and Educational Institution

- Position of the contact persons
- Contact details (email address, telephone number)

B. Version number and version date

The most recent version number of the Privacy Annex and its date are recorded here.

C. General information

This includes information about:

- Name of the product and/or service
- Name of the Processor and its business location details
- Link to the Supplier (website/URL)
- Link to the product page (website/URL)
- Brief explanation of the product and/or service and how it works
- Target group (primary education/secondary education/special education/special secondary education/senior secondary vocational education)
- Users (Educational Participants/parents/carers/employees)

D. Description of specific products and/or services

This section consists of:

a. a description of products and/or services and related Processing operations that form an inseparable part of the product and/or service offered, including the links and exchanges with third parties;

b. a description of additional optional products and/or services and related Processing operations offered by the Processor, including links and exchanges with third parties.

E. Purposes of the Processing of Personal Data

This section records which purposes, as set out in Article 5 of the Privacy Covenant, apply to the Processing of Personal Data in the specific products and/or services.

F. Categories of Personal Data including retention periods

This section consists of:

1. a description of the categories of Data Subjects (e.g. Educational Participants, parents/carers, employees) whose Personal Data are processed, and the categories of Personal Data of these Data Subjects to be processed, and
2. specific retention periods for Personal Data to be applied by the Processor (or assessment criteria for determining this).

G. Location of storing and Processing of Personal Data

The one or more places and/or countries of storing and Processing of Personal Data are recorded under G.

H. Subprocessors

The Processor lists which Subprocessors it uses at the time of entering into the Data Processing Agreement here.

Explanatory notes to the requirements for Annex 1

A. Contact details of the Processor and Educational Institution

To comply properly with the arrangements recorded in the Data Processing Agreement and Annexes, the Parties need to be able to contact each other quickly with questions and comments. The Privacy Annex therefore includes information on both Parties' contact persons. This includes the contact person's position and contact details (e.g. email address and telephone number).
It is important that the Educational Institution's contact person is authorised/mandated to give assignments and Instructions to the Processor on the Educational Institution's behalf.

B. Version number and version date

The Privacy Annex must always have a version number and a version date, so that the most recent and applicable version is always clear to the Parties.

C. General information

The general information includes the name of the product and/or service, the Processor's name and business location details, a link to the Processor's website and/or to the website of the product and/or service, a brief explanation of the product and/or service and how the product and/or service work(s), the target group (primary education/secondary education/special education/special secondary education/senior secondary vocational education), and the intended users (Educational Participants/employees of the Educational Institution/parents/carers).

D. Description of specific products and/or services

Under this heading, the Processor describes the specific products and/or services. Links and exchanges with third parties are also described.
The Processor also distinguishes between products and/or services and related Processing operations that form an inseparable part of the product and/or service offered and additional optional products and/or services and related Processing operations that the Processor offers.

An example of this would be an optional application for parent communication in a pupil administration system. The purpose of this description is for the Educational Institution to give informed consent for the additional products and/or services and related Processing operations that are not an inseparable part of the product and/or service offered.

The Educational Institution must state under D. whether it gives approval for these products and/or services based on the included information. By giving this approval, the Educational Institution also instructs the Processor to process personal data for the purpose of these products and/or services. This can be done by recording the choice in writing in the Privacy Annex or in another written way.

The instruction can also be given by the Educational Institution activating the product and/or service in practice, for example by switching a product and/or service on or off. The Educational Institution making a choice in this way must be able to do so based on previously provided information (such as included in this Privacy Annex).

E. Purposes of the Processing of Personal Data[1]

Under the Privacy Covenant, Educational Institutions may Process Personal Data specifically for the purposes set out in Article 5 of the Privacy Covenant.

The Processor must thus be aware that when the Educational Institution uses the products and/or services offered, it must be able to process the data within the scope of these purposes.

The following purposes are stated in Article 5:
Educational Institutions Process Personal Data with the help of Digital Educational Resources for the purpose of providing education, including preparing, implementing, evaluating and supporting education and/or the educational process, and supervising and monitoring Educational Participants (in their learning process). More specifically, Educational Institutions Process Personal Data with the help of Digital Educational Resources mainly for:

a. storing learning outcomes and test results;
b. returning learning outcomes and test results to the Educational Institution;
c. assessing learning outcomes and test results to be able to obtain course and test materials that are tailored to an Educational Participant's specific learning needs;
d. analysing and interpreting learning outcomes and test results;
e. exchanging learning outcomes and test results between Digital Educational Resources;
f. arranging and adjusting timetables;
g. tracking an Educational Participant's personal circumstances (including their medical information) and how that affects them receiving education;
h. guiding and supporting teachers and other employees in the Educational Institution;
i. communicating with Educational Participants, parents and employees of the Educational Institution;
j. monitoring and accountability, particularly performance and other measurements of the Educational Institution, quality assurance, satisfaction surveys, research into the effectiveness of education and/or a form of education or the support offered to Educational Participants in appropriate education;
k. insofar as necessary and permitted by law, exchanging Personal Data with Third Parties, including:
    - supervisory authorities and healthcare institutions in relation to them performing their statutory and other duties;
    - partnerships in the context of appropriate education and regional cooperation;
    - parties involved in filling traineeships, practical training or work experience places;
    - providing Personal Data to Educational Institutions in the event of transfers between educational institutions and further education;
    - providing Personal Data to another party on the Educational Institution's instructions;
l. taking delivery of/being able to use Digital Educational Resources in accordance with the arrangements made between the Educational Institution and the Supplier;
m. gaining access to the Digital Educational Resources offered and external information systems, including identification, authentication and authorisation;
n. securing, controlling and preventing misuse and improper use, and avoiding inconsistency and unreliability in the Personal Data Processed with the Digital Educational Resources;
o. bringing continuity, improvements and proper functioning to the Digital Educational Resource on the Educational Institution's instructions in accordance with the arrangements made between the Educational Institution and the Supplier, including arranging maintenance, making backups, introducing improvements, for example after errors or inaccuracies have been detected, and obtaining support;
p. making it possible for the Educational Institution to provide anonymised or pseudonymised Personal Data for scientific research or statistical purposes relating to the Educational

[1] For Educational Institutions, the explanatory notes summarise the relationship between the processing purposes listed in section E and the main and other business functions in the Primary and Secondary Education Reference Architecture (FORA). Educational Institutions can use this summary in the explanatory notes to select the specific processing purposes that apply, supplemented by the main and other business functions in the FORA.

Institution's learning process, policy or their respective optimisation, which is implemented under strict conditions comparable to existing codes of conduct in the area of research and statistics;

q. making it possible for the Educational Institution to provide anonymised Personal Data for research and analysis purposes in order to improve the quality of education;
r. providing Personal Data insofar as necessary to meet the statutory requirements set for Digital Educational Resources;
s. handling disputes;
t. financial management;
u. implementing or applying a provision of a European Union or Member State law or regulation.

The objectives that apply to the product and/or service are included in this section so it is clear in arrangements between the Educational Institution and the Processor that these objectives form the basis for both Parties when data Processing occurs with the help of the products and/or services to be provided.

F. Categories of Personal Data including retention periods

1. Data Subjects and categories of Personal Data

The Educational Institution and the Processor must jointly complete this section. This includes information on which categories of Data Subjects and which categories of Personal Data are processed in the product and/or service.

First, this will concern the categories of Personal Data relating to the Educational Participant (in this case, the pupils or students of the Educational Institution). The Processing operations also record data on other Data Subjects (such as employees of the Educational Institution or parents). Although the Privacy Covenant does not primarily focus on these Data Subjects, it is important – partly in connection with Data Breaches – that the Parties name these categories of Data Subjects, including the Personal Data relating to them.

These are the possible categories of Personal Data:

Data Subject: Educational Participant	**Category of Personal Data:**
	Contact details
	Citizen service number (BSN) or personal identification number (PGN)
	Educational Participant number
	ECK-iD
	Nationality
	Date of birth
	Place of birth
	Financial data for the purpose of calculating, recording and collecting money and contributions
	Health data*
	Religion*
	Study progress
	Educational Institution
	Visual material
	User data (data on user behaviour, such as login time, opening of documents, language settings, and so on)
	Other personal data, to be completed by the Parties

*These are special personal data that may not be processed unless the requirements of the GDPR and the Dutch General Data Protection Regulation (Implementation) Act are fulfilled.

Data Subject: parents/guardian/carers	**Category of Personal Data:**
	Contact details
	Financial data for the purpose of calculating, recording and collecting money and contributions
	User data (data on user behaviour, such as login time, opening of documents, language settings, and so on)
	Other personal data, to be completed by the Parties

Data Subject: employee of Educational institution	**Category of Personal Data:**
	Contact details
	Educational Institution
	Visual material
	User data (data on user behaviour, such as login time, opening of documents, language settings, and so on)
	Other personal data, to be completed by the Parties

2. Retention periods

This section must also record the retention period of the Personal Data or the criteria based on which the retention period is determined. The retention periods depend on the purpose for which and the Personal Data that are processed. The information on aanpakibp.kennisnet.nl, for example, can be used to determine the retention period(s) of Personal Data.

G. Location of storing and Processing of Personal Data

If Personal Data are transferred to a third country outside the European Economic Area or to an international organisation, this must be stated in the Privacy Annex on the basis of Article 10 of the Model Data Processing Agreement, including a list of the countries where, or international organisations by which, the Personal Data are processed.

It must also be explained how the conditions for transferring Personal Data to third countries or international organisations are ensured on the basis of the GDPR. Possible safeguards include an adequacy decision by the European Commission for the country concerned or – in the absence of such a decision – Standard Contractual Clauses (SCCs) with, if necessary, sufficient additional measures to ensure the security of the transfer.

The Processor may transfer only if the Educational Institution has given its specific Written consent for this purpose.

H. Subprocessors

By signing the Data Processing Agreement, the Educational Institution gives its general written consent to hire a Subprocessor. The Privacy Annex lists the Subprocessors that the Processor already uses when the Data Processing Agreement is concluded and which service the Subprocessor provides. After entering into the Data Processing Agreement, the Processor may use Subprocessors other than those listed in the Privacy Annex, provided that prior notice is given to the Educational Institution and the Educational Institution can object within a reasonable period.

Annex 1 (Privacy Annex) is part of the arrangements made in the Privacy Covenant for Digital Educational Resources 4.0, an initiative of the Primary Education Council, Secondary Education Council, Association of Vocational Education and Training Colleges, the various chain parties involved (MEVW, KBb-e and VDOD) and the Ministry of Education, Culture and Science. More information is available here: https://www.privacyconvenant.nl/.

Requirements for Annex 2: the Security Annex

Under the GDPR and Articles 7 and 8 of the Model Data Processing Agreement, the Processor must implement appropriate technical and organisational measures to secure the Processing of Personal Data and demonstrate these measures. This Annex briefly describes and summarises those measures.

Parties to the Privacy Covenant affiliated with a sector organisation that is a joint Initiator of the Privacy Covenant (MEVW, VDOD, KBb-E) use the Security Annex that has been drawn up by this sector organisation, if available. The sector models can be found on www.privacyconvenant.nl

The Security Annex [version number and date of last update] for [name of product/service] must cover at least the following topics.

A. Measures to protect the Personal Data against accidental or unlawful destruction, alteration, storage, access or disclosure

- The Processor has an appropriate policy for securing the Processing of the Personal Data, which is periodically evaluated and – if necessary – adapted.
- The Processor implements measures so that only authorised employees can access the Processing of Personal Data under the Data Processing Agreement through an authorisation system. Under this system, employees have no access to more data than is strictly necessary for their position.
- The Processor has an information security coordinator to identify and list risks relating to the Processing of Personal Data, raise security awareness, monitor arrangements and implement measures to ensure compliance with the information security policy.
- Information security incidents are documented and used to optimise the information security policy.
- The Processor has established a process for communicating about information security incidents.
- The Processor concludes non-disclosure agreements with employees and makes information security arrangements.
- The Processor raises awareness and promotes education and training in relation to information security.

B. Measures to secure the Personal Data and to ensure the continuity of resources, the network, the server and the application

The report on the AIC classification, the level of compliance and the explanation of any deviations from the standards is set out below. In principle, the Processor uses the 'ROSA Certification Scheme for Information Security and Privacy' (on www.edustandaard.nl) as an assessment framework for this purpose and to create a solid basic level of information security and privacy.

Test form	[Self-assessment/internal audit/peer review/external audit]		
Test administrator	[Organisation, name and position of administrator]		
Login page	[If applicable, the URL of the login page]		
AIC classification	[Availability=L/M/H, Integrity=L/M/H, Confidentiality=L/M/H]		
Category	**Measures**	**Compliance**	**Explanation**
		[Fulfilled/ not fulfilled/ alternative measure]	[If not fulfilled, state how/ when this will be rectified. If an alternative measure applies, describe it.]
Availability	Design		
	Capacity management		
	Maintenance		
	Testing		
	Monitoring		
	Recovery		
Integrity	Traceability (users)		
	Backup		
	Application controls		
	Irrefutability		
	Traceability (technical management)		
	Integrity check		
	Irrefutability		
Confidentiality	Data life cycle		
	Logical access		
	Physical access		
	Network access		
	Separation of environments		
	Transport and physical storage		
	Logging		
	Dealing with vulnerabilities		

C. Arrangements for reporting security incidents and/or Data Breaches

The Processor has a procedure for monitoring and identifying incidents and for reporting Data Breaches and/or security incidents. In such a case, the Processor must provide the Controller with the following information:

- the characteristics of the breach, such as date and time of discovery, duration of the breach, summary of the breach including the nature of the breach and the nature and description of the security incident (what aspect of security does it relate to, how did it occur, does it relate to reading, copying, altering, deleting/destroying and/or theft of personal data?);
- the cause of the breach;
- how the breach was discovered;
- the measures implemented to address the breach and to prevent any damage, including continued and future damage;
- whether the data involved in the breach was encrypted, hashed, and so on;
- naming the group(s) of Data Subjects that could be affected by the incident, and the numbers and size of the group of Data Subjects;
- what the possible consequences of the breach are for the Educational Institution and the Data Subject(s), including, if possible, an estimate of the risk of the consequences for the Data Subject(s);
- the quantity and type of Personal Data involved in the breach (in particular, special data such as data concerning health or religion, or data of a sensitive nature, including access or identification data, financial data or learning achievements).

If an actual or suspected security incident and/or Data Breach occurs, the Educational Institution and the Processor can contact each other, in principle, by email using the contact details below or the contact details included in Annex 4.

	Name and position of the contact person for security incidents/Data Breaches	**Contact details (email and telephone number)**
Processor	*[name and position of Processor's contact person]*	*[Processor's contact details]*
Educational Institution	*[idem for Educational Institution or see Annex 4]*	*[idem or see Annex 4]*

Explanatory notes to the requirements for Annex 2

The Processor must demonstrate to the Educational Institution whether and how appropriate technical and organisational measures have been implemented to ensure and to be able to demonstrate that the Processing occurs in accordance with the GDPR and the Data Processing Agreement.

The Processor must first indicate (under A) whether and how the minimum security measures, as referred to in Article 32 GDPR, are fulfilled.

As for the classification of availability, integrity and confidentiality (AIC classification), the Processor must explain in the Security Annex whether the measures appropriate to the AIC classification of the product and/or service are fulfilled. The Processor records this in the table under B of the Security Annex.

For the purpose of making the AIC classification and applying and demonstrating the appropriate technical measures, the Processor can use the 'ROSA Certification Scheme for Information Security and Privacy' (on www.edustandaard.nl). This scheme provides a classification tool and an assessment framework that describes specific measures for an ICT application for each information security aspect.

The Processor may also use other certification mechanisms and/or internationally or nationally recognised norms and standards for information security to complete the table under b., provided that these offer an equivalent or higher level of security and that the measures the Processor implements are made clear to the Educational Institution.

The final section of the Security Annex (under C) records the arrangements for how the Parties deal with Data Breaches and security incidents.

Annex 2 (Security Annex) is part of the arrangements made in the Privacy Covenant for Digital Educational Resources 4.0, an initiative of the Primary Education Council, Secondary Education Council, Association of Vocational Education and Training Colleges, the various chain parties involved (MEVW, KBb-e and VDOD) and the Ministry of Education, Culture and Science. More information is available here: https://www.privacyconvenant.nl/.

Requirements for Annex 3: the Amendments Annex

MANDATORY DESCRIPTION OF THE NECESSARY DEVIATIONS FROM THE MODEL DATA PROCESSING AGREEMENT

The Amendments Annex [version number and date of last update] for [name of product/service] must include a summary of the deviations referred to in Article 14, paragraph 2 of the Model Data Processing Agreement and the reasons for them.

The Parties record necessary deviations from the Model Data Processing Agreement in this Annex. They also note which article is concerned and whether it is an amendment or an addition. The old and new texts are then included, with the amendments and additions underlined in the new text. This is followed by the motivation for the deviation. Example:

The Parties have agreed on the following amendments:

1. Description of necessary deviations from the Model Data Processing Agreement	
Article number	
Amendment or addition?	
Current text of the article	
New text of the article (underline amendments and additions)	
Reason for amendment or addition (necessity and motivation)	

Explanatory notes to the requirements for Annex 3

The Privacy Covenant stipulates that Educational Institutions and Processors must use the Model Data Processing Agreement when making arrangements for the Processing of Personal Data with the help of Digital Educational Resources.

Given the number of provisions that are either prescribed by law or which the Dutch Data Protection Authority states must be included in a data processing agreement, the scope for deviating from the provisions of the Model Data Processing Agreement is limited.

However, if a specific article of the Model Data Processing Agreement cannot be used because of certain circumstances, this article can be deviated from only in writing and if reasons are stated. This is recorded in Article 4, paragraph 2 of the Privacy Covenant and Article 14, paragraph 2 of the Model Data Processing Agreement. This concerns only deviations or additions to the articles of the Model Data Processing Agreement, and not additions and/or amendments to Annexes 1 and 2 to the Model Data Processing Agreement.

This Annex 3 must a include motivation as to why adaptation is necessary in the specific case.

Annex 3 (Amendments Annex) is part of the arrangements made in the Privacy Covenant for Digital Educational Resources 4.0, an initiative of the Primary Education Council, Secondary Education Council, Association of Vocational Education and Training Colleges, the various chain parties involved (MEVW, KBb-E and VDOD) and the Ministry of Education, Culture and Science. More information is available on www.privacyconvenant.nl.