Data Processing Agreement

Processor: Puzzel.org

This document contains the Data Processing Agreement and its two Schedules. The Schedules are already complete; the School fills in its own details on the first page and signs at the end.

DATA PROCESSING AGREEMENT

Puzzel.org — for schools and other educational institutions

Version **1.0**, date of last amendment **20 September 2026**.

> This Agreement is offered by the Processor. It does not need to be negotiated: a School that wishes to use it signs it as it stands. Schedules 1 and 2 are part of it and are already complete.

Parties

(1) The Processor

Name	Puzzel.org
Legal form	Sole proprietorship under the laws of the Netherlands
Address	Sneekermeer 13, 3825 XT Amersfoort, the Netherlands
Represented by	Daan Weustenraad, owner
Contact for this Agreement	daan@puzzel.org

(2) The School

Name	.....
Address	.....
Represented by	.....
Contact for this Agreement	.....

Together referred to as the **Parties**.

Recitals

A. The School uses the online platform Puzzel.org to create and share educational activities, and to see the results of those activities.

B. In doing so, the School determines the purposes and means of the Processing of Personal Data and is therefore the **controller** within the meaning of Article 4(7) GDPR. Puzzel.org Processes that Personal Data on the School's behalf and is therefore the **processor** within the meaning of Article 4(8) GDPR.

C. Article 28(3) GDPR requires that this relationship be governed by a contract. This Agreement is that contract.

D. This Agreement is modelled on the Dutch education sector's *Model Verwerkersovereenkomst 4.0*, published by the Privacyconvenant Onderwijs (privacyconvenant.nl), and Schedules 1 and 2 follow that sector's templates. A Dutch School may prefer to use the sector agreement itself; this Agreement exists for Schools outside the Netherlands, for whom the Dutch text is not usable.

---

1. Definitions

Terms defined in the GDPR have the meaning given there. In addition:

Term	Meaning
Agreement	This Data Processing Agreement, including its Schedules.
Data Subject	A person whose Personal Data is Processed — in practice a Student or a member of the School's staff.
GDPR	Regulation (EU) 2016/679.
Personal Data	Personal data within the meaning of Article 4(1) GDPR that the Processor Processes on the School's behalf under the Service Agreement.
Personal Data Breach	A breach within the meaning of Article 4(12) GDPR.
Processing	As defined in Article 4(2) GDPR.
Service Agreement	The agreement under which the School uses the Puzzel.org platform, including the published terms of service.
Services	The Puzzel.org platform and everything the Processor provides under the Service Agreement.
Student	A person taking part in education at the School.
Sub-processor	A third party engaged by the Processor to Process Personal Data on the School's behalf.

2. Subject matter, nature, purpose and duration

2.1 The subject matter, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subject are set out in **Schedule 1**.

2.2 This Agreement takes effect on the date of the last signature and lasts as long as the Service Agreement. It ends when the Service Agreement ends, subject to clause 10.

2.3 Where this Agreement and the Service Agreement conflict on a matter of data protection, **this Agreement prevails**. Where this Agreement and a Schedule conflict, this Agreement prevails.

3. Instructions

3.1 The Processor Processes Personal Data **only on the School's documented instructions**, including as regards transfers to a third country, unless required to do otherwise by Union or Member State law. In that case the Processor informs the School of that legal requirement before Processing, unless that law prohibits it on important grounds of public interest.

3.2 The Service Agreement, this Agreement and its Schedules, together with the choices the School and its teachers make in the platform itself, constitute the School's documented instructions. Configuring an activity is an instruction: whether results are recorded, which registration fields a Student is asked for, whether an activity is shared publicly, and whether scores are sent to the School's own systems are all decisions the School makes and the Processor carries out.

3.3 The Processor **does not Process Personal Data for its own purposes**. It does not sell Personal Data, does not use it for advertising, does not use it to build a profile of a Data Subject, and does not use Student Personal Data to train or improve artificial-intelligence models.

3.4 The Processor immediately informs the School if, in its opinion, an instruction infringes the GDPR or other data protection law.

4. Confidentiality

4.1 The Processor ensures that persons authorised to Process the Personal Data are bound by an appropriate duty of confidentiality.

4.2 The Processor is a sole proprietorship. **The owner is the only person with access to the production environment**, and is bound by this clause personally. Where that concentration of access matters to the School's own risk assessment, it is stated in Schedule 2.

5. Security

5.1 The Processor implements appropriate technical and organisational measures under Article 32 GDPR. Those measures, and the points at which they fall short of the sector norm, are set out **in full and without omission in Schedule 2**.

5.2 The School acknowledges that it has read Schedule 2 and has taken its contents into account in deciding to use the Services. Schedule 2 states plainly which measures are met, which are not, and which are replaced by an alternative measure.

5.3 The Processor may change a measure, provided the level of protection is not reduced. If the Processor becomes aware that the level of protection is no longer appropriate, it informs the School.

6. Sub-processors

6.1 The School gives the Processor **general written authorisation** to engage Sub-processors. The Sub-processors engaged at the date of this Agreement are listed in Schedule 1, section H, with what each one does, which Personal Data it receives and where it Processes that data.

6.2 The Processor imposes on each Sub-processor, by contract, data protection obligations that are **no less protective** than those in this Agreement, and remains **fully liable** to the School for the performance of that Sub-processor's obligations.

6.3 The Processor informs the School of any intended addition or replacement of a Sub-processor **at least thirty (30) days in advance**, by email to the contact named above. The School may object on reasonable data protection grounds within that period. If the Parties cannot resolve the objection, the School may terminate the Service Agreement with respect to the affected Services, without penalty, and clause 10 applies.

7. Assistance to the School

7.1 **Data Subject rights.** Taking into account the nature of the Processing, the Processor assists the School by appropriate technical and organisational measures in fulfilling its obligation to respond to requests under Chapter III GDPR. In practice the platform lets a teacher see, export, correct and delete the results and registrations of their own

activities directly, which will answer most requests without the Processor's involvement. Where it does not, the Processor assists on request.

7.2 If a Data Subject approaches the Processor directly, the Processor does not respond on the merits but forwards the request to the School without undue delay.

7.3 **Articles 32 to 36.** The Processor assists the School in ensuring compliance with its obligations on security, breach notification, data protection impact assessments and prior consultation, taking into account the nature of the Processing and the information available to the Processor.

7.4 The Processor has not appointed a data protection officer and is not required to do so under Article 37 GDPR. The contact point for all matters under this Agreement is the person named in the Parties table.

8. Personal Data Breach

8.1 The Processor notifies the School of a Personal Data Breach **without undue delay, and in any event within forty-eight (48) hours of becoming aware of it**, by email to the contact named above.

8.2 That period is set so that the School can meet its own 72-hour obligation under Article 33(1) GDPR. It does not depend on the Processor first establishing the full extent of the breach; an incomplete notification within the period is preferred to a complete one after it.

8.3 The notification contains the information listed in **Schedule 2, section C**, to the extent known, and is supplemented as more becomes known.

8.4 The Processor **does not notify the supervisory authority or the Data Subjects** on the School's behalf. That decision and that obligation are the School's.

8.5 The Processor keeps a record of Personal Data Breaches and of incidents of significance, and makes it available to the School on request.

9. Audit

9.1 The Processor makes available to the School all information necessary to demonstrate compliance with Article 28 GDPR. Schedules 1 and 2 are the first and fullest part of that information, and the Processor maintains them.

9.2 The Processor allows for and contributes to audits, including inspections, conducted by the School or an auditor it mandates. The School gives at least thirty (30) days' notice, audits at most once in any twelve-month period unless there has been a Personal Data Breach, and bears its own costs. The Processor may require that the auditor sign a confidentiality undertaking.

9.3 The Processor has **not** been independently certified or audited by a third party. Schedule 2 is a self-assessment against a recognised sector scheme, made by the owner, and says so. The School should weigh that when deciding how much assurance it needs.

10. Return and deletion

10.1 Personal Data is retained as described in **Schedule 1, section F.2**. In summary: data is kept until the School or its teacher deletes it — the platform applies no automatic expiry — and a teacher may delete any result, registration or account at any time.

10.2 On termination of the Service Agreement, the Processor, at the School's choice, returns the Personal Data or deletes it. The School makes that choice in writing. The Processor acts on it **within thirty (30) days of receipt**.

10.3 If the School makes no choice, the Processor retains the Personal Data until the School requests otherwise, so that no data is lost by silence. The Processor does not use retained data for any purpose other than storage.

10.4 The Processor may retain Personal Data where Union or Member State law requires it. In practice this concerns invoicing and payment records, which are kept for **seven (7) years** under Dutch tax law. Schedule 1, section F.2 lists the records that survive deletion of an account, and the School should read that list rather than assume deletion is total.

11. International transfers

11.1 Personal Data is Processed in the European Union and in the United States. Which Processing takes place where is set out in **Schedule 1, section G**, per Processing operation, and is not left general.

11.2 The School gives its **specific written consent**, by signing this Agreement, to the transfers described in Schedule 1, section G.2.

11.3 Each transfer to a third country is covered by an appropriate safeguard under Chapter V GDPR — the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), the EU–US Data Privacy Framework, or both. Schedule 1, section G.2 names the safeguard for each transfer and gives the URL at which the School can read it.

11.4 **A School that requires all Processing to take place within the EEA cannot use the Services.** Some platform-wide Processing takes place in the United States for every account, whichever storage region the account uses, and some Sub-processors do not offer EU data residency on the plan in use. Schedule 1, section G states which.

12. Liability

12.1 The liability of the Parties is governed by the Service Agreement, save that no limitation in the Service Agreement restricts a Data Subject's rights under Article 82 GDPR or a supervisory authority's powers.

12.2 Each Party bears its own administrative fines.

13. Final provisions

13.1 This Agreement is governed by the law of the Netherlands.

13.2 Disputes are submitted to the competent court in the district where the Processor is established, unless mandatory law provides otherwise.

13.3 Amendments are valid only in writing and signed by both Parties. The Processor may update Schedules 1 and 2 to reflect a change in the Services or in its Sub-processors, subject to clause 6.3; it informs the School of a material change and publishes the current version.

13.4 If a provision is invalid, the remainder stays in force and the Parties replace the invalid provision with one that approaches its purpose as closely as possible.

Schedules

Schedule 1	Details of Processing — services, purposes, categories of Personal Data, retention, storage locations, transfers, Sub-processors
Schedule 2	Security measures — the measures taken, the classification, and the points at which the Processor does not meet the sector norm

Both Schedules form an integral part of this Agreement.

Signatures

The Processor	**The School**
Puzzel.org	.....
Name: Daan Weustenraad	Name: .....
Position: owner	Position: .....
Date:	Date: .....
Signature:	Signature: .....

SCHEDULE 1: DETAILS OF PROCESSING — Puzzel.org

A. Contact details

For questions or comments about these Details of Processing or about the way this product and/or service works, please contact:

	Role and name of contact person	Contact details
Processor	Owner and sole contact person — Daan Weustenraad	daan@puzzel.org No telephone number is published; contact is by email.
School*	[To be completed by the School]	[To be completed by the School]

* This contact person is authorised/mandated to give orders and Instructions to the Processor on behalf of the School.

B. Version number and version date

Processor: **Puzzel.org**. Version **1.0**, date of last amendment **20 September 2026**.

C. General information (completed by the Processor)

Field	Entry
Name of product and/or service	Puzzel.org
Name and establishment details of the Processor	Puzzel.org, Sneekermeer 13, 3825XT Amersfoort, the Netherlands. Chamber of Commerce number 66090091, VAT number NL002191535B44. Puzzel.org — sole proprietorship, registered in the Commercial Register of the Netherlands Chamber of Commerce under number 66090091
Link to the Supplier (website/URL)	https://puzzel.org
Link to the product page (website/URL)	https://puzzel.org/nl — overview of the activity types: https://puzzel.org/nl/activities — supplier information for IT departments: https://puzzel.org/nl/vendor-info
Brief explanation and operation of the product and/or service	Puzzel.org is a web application with which a teacher creates interactive learning activities — crosswords, word searches, quizzes, memory games, escape-room-style assignments and some thirty other types (36 activity types in all) — and shares them with students through a link, a QR code, a join code, an embed code or the school's own virtual learning environment. There is no installation: everything runs in the browser. By default a student plays anonymously and nothing about the student is recorded. A teacher can switch on two separate settings per activity: tracking results and requiring registration. Only then is Personal Data of students Processed, and only the fields the teacher selects from a fixed list.
Target group (po/vo/(v)so/mbo)	Primary education (po), secondary education (vo), (special) secondary education ((v)so) and senior secondary vocational education (mbo). The product is not limited to one sector and is also used in higher education; that falls outside the Dutch sector agreement.

Field	Entry
Users (Students/parents/guardians/staff)	Students and staff of the School. **Parents/guardians are not users**: the platform has no parent role, no parent account and no parent communication.

D. Description of specific products and/or services (completed by the Processor)

D.1 Products and/or services and the associated Processing that form an inseparable part of the product and/or service offered

Description of product and/or service	Associated Processing
1. Teacher account and signing in	Creating and managing an account for a member of the School's staff: first name, email address and language preference. Signing in with an email address and password, or with the Google or Microsoft account the school already manages. Authentication runs through Google Firebase Authentication; the password is managed by Firebase and does not enter the Puzzel.org database. Connection with a third party: Google Firebase Authentication (and, with SSO, the school's identity provider).
2. Creating, storing and managing activities	Storing the content the teacher creates: questions, answers, clues, texts, settings, folders and templates. This content is filled in freely by the teacher ("open fields") and may therefore contain Personal Data that the Processor cannot limit in advance.
3. Uploading files	Storing images, audio fragments and documents that the teacher uploads, in Amazon S3, under a key that includes the teacher's account id. **Note: uploaded files are given a publicly readable URL.** Anyone who has the URL can retrieve the file. Uploaded documents (PDF) are checked for malware in quarantine before publication.
4. Playing an activity	A player is signed in anonymously to Firebase Authentication — also without an account — so that the application has a temporary player id. Without the optional services under D.2 no data about the player is stored: no name, no score, no result. Progress within a single session stays in the browser.
5. Security and abuse prevention	Rate limiting on public endpoints, based on the player id and on a **SHA-256 hash of the IP address salted with a secret**; the IP address itself is not stored. Counting the number of game sessions per month for the subscription limit.
6. Availability, maintenance and support	Hosting and delivery of the application through Vercel; storage and management of the data in Google Firebase Realtime Database; email to the account holder about the account and about outages through SendGrid; support by email through daan@puzzel.org.
7. Web fonts	Every page — **including a play page that a student opens** — loads its fonts from Puzzel.org's own environment. The font files are part of the application and are served from the same domain, so no third-party font service is contacted and nothing about the visitor reaches one. Until 20 September 2026 the fonts came from Google Fonts; that connection has been removed.

D.2 Additional optional products and/or services and associated Processing offered by the Processor

In the last column the School indicates whether it agrees to the additional optional products and/or services and the associated Processing. Every service below is **off** by default and only becomes active because the teacher or the school switches it on.

Description of product and/or service	Associated Processing	Agreement of the School
8. Tracking results (off by default)	Recording per player: the time of play, the time spent, the progress, the answers given, which answers were correct, any score and the number of attempts. The result is stored under the teacher's account, per activity and per player. A player can read only their own result; the teacher reads all results for their own activity.	□
9. Registration of players (off by default)	The player fills in a form before or after playing. The teacher chooses which fields are asked from this fixed list: name, first name, surname, email address, telephone number, student number, staff number, organisation name, class, country, "other information", password and one self-formulated question. By default only a first name is asked for. Activities created before 26 August 2026 still carry the older default selection of name, email address and password. In either case the teacher decides the final selection. The fields "other information" and the self-formulated question are open fields. **Note:** if the teacher chooses the *password* field, the student creates a real, permanent user account with Firebase Authentication together with an account record of their own at Puzzel.org (first name, email address, language preference). With the other fields the player remains anonymous. The password entered is not stored in the result.	□
10. Classroom leaderboard (off by default)	Showing players with their time or score to other players of the same activity. The leaderboard is a restricted view: only one name field is published, and if that is an email address or telephone number it is masked. The full registration form does not appear in it.	□
11. Single sign-on for players (off by default)	The player signs in with a Google or Microsoft account, from the school's own portal, or through OIDC against an issuer permitted for that account. The account id, and depending on the setting the name and the email address, are kept with the result.	□
12. Puzzel LMS — classes and courses	Recording a class list under the teacher's account: per student a first name, an optional surname, an optional email address, an order, a hash of a self-chosen password and, after signing in with SSO, the provider and the email address of that account. This is the only Processing in which a real class list is stored at the Processor. Courses may contain documents and videos belonging to the teacher.	□
13. Grade integration with Google Classroom	The teacher connects their own Google account. Stored are: the Google account id and the email address of the teacher, the permissions granted and an encrypted refresh token; the key with which that token is encrypted stays on the server. Per assignment and per student: the student's Google account id, the id of the submission, the grade last sent and the time. Sent to Google are: the assignment details (title, description, the link to the activity, the maximum number of points, the due date) and the student's **grade**. The permissions requested are limited to: reading the teacher's courses, managing student submissions on assignments, and the email address of the connected account; **no** class list is retrieved.	□
14. Grade integration through LTI 1.3 with the school's own learning environment (Moodle, Canvas, Brightspace and comparable)	When an activity is started from the learning environment, Puzzel.org receives from the platform's signed identity message: the platform id of the user, and in so far as the school shares them the name and the email address, plus the role. No Puzzel.org account is created for the student. If the teacher has grades written back, the platform id, the address of the grade column and the grade last sent are kept per student, and only the **grade** is sent to the platform.	□
15. Joining with a code (join PIN)	An activity is given a temporary numeric code that points to the ordinary play URL. Only the link between the code and the activity is stored; nothing is recorded about the student typing it in. The code expires and is cleaned up by a daily task.	□
16. School account and shared library	Several teachers work under one school account. Recorded are the link between the teacher and the school and, with a shared library, a temporary editing lock indicating who is editing an activity at that moment.	□

Description of product and/or service	Associated Processing	Agreement of the School
17. AI assistant for the teacher	What the teacher types or uploads is sent to an external AI provider to have content generated. **OpenAI** receives free text: a theme, a list of answers, or — when translating an activity — the full text of that activity (up to around 120,000 characters). **Google Gemini** receives images and complete documents: an uploaded PDF, Word file or photograph of a worksheet from which exercises are distilled, and images that are to be edited. If a teacher uploads a worksheet or a photograph containing Personal Data, that data goes along with it. The question and the answer are also kept under the teacher's account.	☐
18. Word check during play (only in the "wordle" activity type)	When a student in this one activity type guesses a word that is neither in the activity's answers nor in the word list supplied, **the word the student typed** is sent to OpenAI with the question whether it is an existing word. The player id is not sent along; OpenAI receives only the single word and the language code. The input is technically limited to one word of letters only, and a word checked earlier is answered from temporary storage without consulting OpenAI. **This is the only Processing in which content entered by a student leaves the platform towards an AI provider.** The School can exclude this by not using the "wordle" activity type.	☐
19. Publishing in the public activity library	The teacher publishes an activity for reuse by others. Only the content of the activity is published; results, registrations, progress and settings for tracking, multiplayer and developers are never copied along.	☐
20. Paid subscription	For a paid subscription the account holder's email address and the account id are passed to Stripe and the institution's invoicing details are recorded (name, address, postcode, town, country, VAT number). Payment card details are Processed solely by Stripe and do not reach Puzzel.org's systems.	☐
21. Public API	An account can create activities from its own systems using a key, at most 10 requests per day per key.	☐
22. Changing the storage region	Moving all account data to the other region (see part G) runs as a background task and requires a paid subscription.	☐

E. Purposes for Processing Personal Data

Processing of Personal Data by means of Digital Educational Resources by Schools takes place for the purpose of providing education, including the preparation, delivery, evaluation and support of education (and the educational process) and the guidance and monitoring of Students (in their learning process). Set out below is which more specific purposes apply to the product or service.

Purpose	Tick if applicable to the product or service
the storage of learning and assessment results	☒
the receipt back by the School of learning and assessment results	☒
the assessment of learning and assessment results in order to obtain learning material and assessment material tailored to the specific learning needs of a Student	☐
analysis and interpretation of learning and assessment results	☒

Purpose	Tick if applicable to the product or service
being able to exchange learning and assessment results between Digital Educational Resources	☒
the arrangement and adjustment of timetables	☐
keeping records of a Student's personal (including medical) circumstances and their consequences for attending education	☐
the guidance and support of teachers and other staff within the School	☐
communication with Students and parents and with staff of the School	☒
monitoring and accountability, in particular for the purposes of: (performance) measurements of the School, quality assurance, satisfaction surveys, research into the effectiveness of forms of education or of the support offered to Students in inclusive education (passend onderwijs)	☐
the exchange of Personal Data with Third Parties, in so far as necessary and legally permitted, including: supervisory bodies and care institutions in the context of carrying out their (statutory) task; partnerships in the context of inclusive education (passend onderwijs) and regional collaborations; parties involved in arranging work placements or work-based learning places; the supply of Personal Data to Schools where a Student transfers between Schools and moves on to further education; the supply of Personal Data to another party on the instruction of the School	☐
having Digital Educational Resources supplied / being able to put them into use in accordance with the arrangements made between the School and the Supplier	☒
obtaining access to the Digital Educational Resources offered, and to external information systems, including identification, authentication and authorisation	☒
the security, monitoring and prevention of abuse and improper use, and the prevention of inconsistency and unreliability in the Personal Data Processed by means of the Digital Educational Resource	☒
the continuity, improvement and proper functioning of the Digital Educational Resource on the instruction of the School in accordance with the arrangements made between the School and the Supplier, including having maintenance carried out, making a backup, making improvements among other things after errors or inaccuracies have been identified, and receiving support	☒
enabling the School to make (anonymised or pseudonymised) Personal Data available for scientific research or statistical purposes for the benefit of (optimising) the learning process or the School's policy, carried out on the basis of strict conditions comparable to existing codes of conduct in the field of research and statistics	☐
enabling the School to make anonymised Personal Data available for research and analysis purposes in order to improve the quality of education	☐
making Personal Data available in so far as necessary to comply with the statutory requirements imposed on Digital Educational Resources	☐
the handling of disputes	☐
financial administration	☒
the implementation or application of a provision or rule of Union or Member State law	☐
other purposes for the benefit of providing education, including the preparation, delivery, evaluation and support of education (and the educational process) and the guidance and monitoring of Students (in their learning process), namely …	☐

Explanatory notes to the purposes ticked.

- *Storage, receipt back, analysis and exchange of learning and assessment results* are ticked because the optional services 8, 13 and 14 provide for them: results are stored, can be viewed and exported by the teacher, and a grade achieved can be written back to Google Classroom or to the school's learning environment. Without those options nothing is stored.
- *Communication* concerns staff only: the platform sends no email to students. The leaderboard (service 10) shows players to each other within the same activity.
- *Financial administration* concerns only the contract details of the School and the account holder, not students' data.
- *Improvement* is ticked solely in the meaning the Dutch sector agreement gives it — maintenance, error correction, backup and support on the instruction of the School. **The Processor does not use Students' Personal Data to train models, nor for product research, nor for statistics across institutions.**
- *Not ticked* are, among other things, adaptive learning material, timetables, medical or guidance data, provision to third parties and research purposes: the product does not offer those functions.

F. Categories of Personal Data including retention periods

F.1 Data Subjects and categories of Personal Data

> **Read this first.** Without the optional services under D.2, Puzzel.org Processes **no** Personal Data of a Student at all: a player is anonymous and nothing about him or her is stored. Everything ticked below is ticked because the teacher *can* switch it on per activity and can then choose the field from a fixed list — not because it is Processed by default.

Data Subject: Student

Category of personal data	Specification	Tick if applicable to the Processing
Contact details	First name(s)	☒ (optional, the registration field first name or name; also from a class list or from an SSO or LTI sign-in)
	Initial(s)	☐
	Surname	☒ (optional, the registration field surname; also from a class list)
	Gender	☐
	Home address	☐
	Postcode	☐
	Town of residence	☐
	Telephone number	☒ (optional, the registration field telephone number)
	Email address (private)	☒ (optional, the registration field email address; the form does not distinguish between private and school)
	Email address (school)	☒ (optional, the registration field email address; also from a class list, from a Google sign-in or from a start out of the learning environment)
Citizen Service Number (BSN) or PGN		☐ — is not asked for and not Processed

Category of personal data	Specification	Tick if applicable to the Processing
Student number	An administrative number that identifies Students	☒ (optional, the registration field student number)
ECK-iD		□ — not supported; there is no Nummervoorziening or KetenID connection
Nationality		□
Date of birth		□
Place of birth		□
Financial data for the purpose of calculating, recording and collecting monies and contributions	Bank account number	□
	Invoicing administration	□
Data concerning health*		□ — is not asked for. **Caveat:** the fields "other information" and the self-formulated registration question are open fields. If the School allows special categories of personal data to be entered in them, that happens under its own responsibility and outside these Details of Processing.
Religion*		□ — likewise
Study progress	Class / year group / ILT code	☒ (optional, the registration field class; also as a class name in Puzzel LMS)
	Examination	□
	Study progress and/or study pathway	☒ (the results of an activity: progress, time spent, score, number of attempts, and the grade achieved where there is a grade integration)
	Support for Students, including individual action plans	□
	Attendance and absence records	□
Organisation of education	Data for the purpose of organising education (such as a timetable) and supplying or making available learning resources	☒ (which activity or course has been assigned to the student, and membership of a class in Puzzel LMS)
Images and video	Photographs and video images (visual material) of the Data Subject with or without sound, of the School's activities	☒ — **not by the student**: a student cannot upload anything. But yes through the teacher placing image or audio material in an activity or course in which students can be seen or heard. That material is given a publicly readable URL (see D.1 under 3).
User data	Diagnostic data, log data, metadata, other namely …	☒ — time of creation and of last play, time spent, progress, version number of the activity, and in the "typing" activity type the characters the student kept missing

Category of personal data	Specification	Tick if applicable to the Processing
	IP address	☒ — **with emphasis on the form.** The IP address is not stored as such. For rate limiting, a SHA-256 hash of the IP address salted with a secret is kept. The IP address itself is Processed in the network traffic and in the logging of the hosting party (Vercel) and of the storage parties; see parts G and H. When feedback or a report about a library item is submitted, the reporter's user agent is included in the email to the administrator.
Other Personal Data, namely		☒ — • the temporary, anonymous player id that every player is given; • **the answers and the free text the student types into an activity** — this is open input and may contain anything the student writes; • a hash of a self-chosen password, if the teacher uses a password field or a class list with passwords; • the account id (and, depending on the settings, the name and email address) of a Google or Microsoft account with which the student signs in; • the user id that the school's learning environment sends along with an LTI start, and the name and email address in so far as the school shares them; • the id of the submission in Google Classroom and the grade last sent; • the organisation name, the country, the staff number and the self-formulated question, in so far as the teacher switches those fields on; • **a user account of their own** at Puzzel.org (first name, email address, language preference) if the teacher uses the *password* registration field — see service 9; • in multiplayer variants: the first name given, the team, the turn order and the answers submitted in the game session.

* These are special categories of Personal Data which may not be Processed unless the requirements of the GDPR and the Dutch GDPR Implementation Act (UAVG) are met.

Data Subject: parent/guardian/carer

No Personal Data of parents, guardians or carers is Processed. The platform has no parent role, no parent account, no parent communication and no field in which parent data is asked for.

Category of data	Specification	Tick if applicable to the Processing
Contact details	First name(s)	☐
	Initial(s)	☐
	Surname	☐
	Form of address, such as gender	☐
	Home address	☐
	Postcode	☐
	Town of residence	☐
	Telephone number	☐
	Email address (private)	☐

Category of data	Specification	Tick if applicable to the Processing
Financial data for the purpose of calculating, recording and collecting monies and contributions	Bank account number	☐
	Invoicing administration	☐
User data	Diagnostic data, log data, metadata, other namely …	☐
	IP address	☐
Other Personal Data, namely:		☐

Data Subject: member of staff of the School

Category of data	Specification	Tick if applicable to the Processing
Contact details	First name(s)	☒ (mandatory when creating an account)
	Initial(s)	☐
	Surname	☒ (optional; is filled from the profile or on SSO)
	Form of address, such as gender	☐
	Email address (school)	☒ (mandatory; is also the sign-in name)
Organisation of education	Timetable	☐
	Guidance data	☐
Images and video	Photographs and video images (visual material) of the Data Subject with or without sound, of the School's activities	☒ — in so far as the member of staff places such material in an activity or course themselves
Usage data	Diagnostic data, such as log data, metadata, other namely …	☒ — language preference, subscription status and date, the number of game sessions this month, the number of AI credits and the AI questions asked together with the answers, and the storage region settings
	IP address	☒ — in the same form and with the same caveat as for the Student above
Other Personal Data, namely:		☒ — • the content the member of staff creates and uploads (open fields: questions, answers, texts, images, audio, documents); • the link to a school account; • the institution's invoicing details and the customer id at Stripe, with a paid subscription; • the Google account id, the email address and an encrypted refresh token where there is a connection with Google Classroom; • a personal API key, if the member of staff uses the public API; • the content of email correspondence with support, in the Processor's mailbox; • feedback and ideas submitted for the roadmap, with name, email address, the page visited, the screen size and the user agent.

F.2 Retention period of the Personal Data or the criteria for determining it

The specific retention periods are determined by the School as Controller, where appropriate on the basis of a proposal by the Processor. Set out below is what the product actually does, and after that the Processor's proposal.

What the product actually does:

Data	Actual behaviour
Activities, results, registrations, class lists, courses	**No fixed retention period.** This data remains until the teacher or the School deletes it. There is no automatic clean-up.
A single result	Deleted as soon as the teacher deletes it.
An activity	On deletion the content, the statistics and the registrations of that activity go with it.
The account	On deletion all data held under the account id is deleted in **both** regions, the uploaded files are deleted from the file storage, the Google Classroom token is revoked at Google, and the sign-in at Firebase Authentication is deleted.
Grades already written to Google Classroom or to the learning environment	Remain there: they belong to the school's grade register.
Multiplayer rooms of the "challenge" type	Are deleted by a daily task once they are **more than 7 days old**.
Multiplayer sessions of the other types and the associated registrations	**Are not cleaned up by any task.** They disappear only when the teacher deletes the activity or the results, or on deletion of the account.
Join codes (join PIN) and LTI hand-over data	An LTI hand-over is single-use and lapses after 5 minutes (start of an activity) or 30 minutes (deep link) respectively; a join PIN lapses at the moment chosen by the teacher. Both are in addition cleaned up by a daily task.
Invitations to a school account	Lapse after 30 days.
Rate limiting (hashed IP addresses)	Lapses with the limit's time window; daily and monthly counters are cleared by the daily and monthly task.
Stored word checks	Lapse after the configured time window.
The email send log and the email queue	Remain in the United States database; this data is **not** affected by deletion of the account.
Payment and invoicing data	The payment administration and the associated accounting records sit outside the account and are **not** affected by deletion of the account.
Feedback and ideas submitted	Contain name, email address, the page visited, the screen size and the user agent, and are **not** affected by deletion of the account.

Retention periods of the Processor. The application enforces no automatic expiry period; the following periods apply:

1. **Accounts, activities, results and registrations** are retained until the teacher or the School deletes them. That can be done at any time, in the application itself. There is no automatic deletion of inactive accounts. The School may specify its own, shorter period in part F.2 and carry it out itself.
2. **After termination of the Data Processing Agreement** (Article 12(2) of the Dutch sector model Data Processing Agreement) — that is: when the School stops using Puzzel.org — the data is deleted within 30 days upon written request, in so far as the School has not already done so itself.
3. **Invoicing and payment data** is retained for seven years (statutory tax retention obligation).
4. **The email send log** is not cleaned up automatically and is deleted on request.

5. **Backups** of the database are made daily by Firebase and retained for 30 days; deleted data may therefore still be present in them for up to 30 days (see Schedule 2).

G. Location of storage and Processing of Personal Data

> **A key point which a School must weigh up explicitly.** Puzzel.org has two independent region settings per account: one for the database and one for the files. A new account is given the region matching the browser's time zone: a browser in a European or African time zone is given **EU**. A Dutch school signing up from the Netherlands therefore ends up in the EU region. The **fallback value remains the United States**, however, and accounts from before the setting was introduced are in the United States. **In addition, a number of platform-wide data collections are always in the United States, also for an EU account** (see below). The School must check the region setting of its account(s) and have it changed if necessary; changing it requires a paid subscription and runs as a background migration.

G.1 Place/country of storage and Processing per Processing

Processing (see part D)	Place/country of storage and Processing of the Personal Data
1, 2, 8, 9, 10, 11, 12, 16 — account, activities, results, registrations, classes, school account (Google Firebase Realtime Database)	**Belgium** if the account is on the EU region; **United States** if the account is on the US region (default and fallback region). The United States instance is in Iowa. According to Firebase's documentation the European instance is in Belgium and the American one in Iowa; the location of an instance cannot be changed (firebase.google.com/docs/database/locations). Google states that Processing by the service may also take place at other Google Cloud locations; the region determines where the data is stored.
1, 4, 11 — authentication (Google Firebase Authentication)	**United States, regardless of the account's region.** Google states that Firebase Authentication runs solely from American data centres and Processes data solely in the United States (firebase.google.com/support/privacy). The region cannot be set. This concerns the teacher's email address and sign-in details, and the anonymous player id.
3 — uploaded images, audio and documents (Amazon S3)	**Sweden (Stockholm)** if the account is on the EU file region; **United States (California)** if it is on the US region. A change to the setting applies only to new uploads; existing files stay where they are.
3 — malware check on documents (AWS GuardDuty Malware Protection for S3)	In the region of the file storage concerned. The malware check applies solely to documents uploaded in the course (LMS) part of Puzzel.org; images and audio are not checked for malware.
5, 6 and all Processing — running the application and the API (Vercel)	**Frankfurt, Germany and Washington D.C., United States.** The functions run in both regions; Vercel sends each request to the region closest to the visitor, so that a request from the Netherlands is normally Processed in Frankfurt. This is a routing rule and not a hard guarantee: in the event of an outage in Frankfurt a request may end up in the other region. This choice of regions was set in Vercel's project settings on 19 September 2026 (Pro subscription) and has been active for both regions since the rollout that same day.
All Processing — platform-wide data collections	**Always the United States**, also for an EU account. Those containing personal data include: the email queue and the email send log (with addressee and name), the index of invitations, the join codes, the registers and hand-over data for the connection with the learning environment (LTI), the payment administration, the rate limiters (with hashed IP addresses), and submitted feedback, ideas and roadmap votes.
6 — email to the account holder (Twilio SendGrid)	**United States.** The service is taken on the standard endpoint; EU data residency exists at Twilio SendGrid only as a paid option with a separate EU subuser and has not been arranged.

Processing (see part D)	Place/country of storage and Processing of the Personal Data
7 — web fonts	Served by the application itself, from the same place as the application (see the Vercel row above). No third party is involved and there is no transfer.
13 — Google Classroom grade integration	Google, worldwide/United States, and the school's own Google Workspace domain.
14 — LTI 1.3 grade integration	The school's learning environment, at the place where the school hosts it.
17, 18 — AI assistant and word check (OpenAI)	**United States.** No region, organisation endpoint or zero-retention option has been set.
17 — AI assistant for images and documents (Google Gemini)	Managed by Google, worldwide. This is the general Generative Language API, not Vertex AI; no region can be set on it and none is set.
17 — searching for stock photographs (Pixabay)	**Germany** (Pixabay GmbH). Only the teacher's search term is sent, from the server; the user's browser does not connect to Pixabay.
20 — payments (Stripe)	Ireland (contracting party Stripe Payments Europe, Limited) with transfer to Stripe, LLC in the **United States** and affiliated undertakings worldwide; Stripe does not offer Processing solely within the EU.

G.2 Transfer outside the EEA

Where several instances of Processing involve a transfer to a country outside the EEA, this table has been used more than once.

Transfer 1 — Google LLC / Google Cloud (Firebase Realtime Database in the US region, Firebase Authentication, Gemini, Google Classroom)

Processing (see part D)	1, 2, 4, 8–12, 13, 17
Description of the transfer outside the EEA	Storage of account data, activities and results in the American database instance (for accounts that are not on the EU region, and for all platform-wide data collections); authentication data; images and documents submitted to Gemini; a student's grade and account id where there is a Google Classroom integration.
Country of Processing or international organisation	United States (Google LLC), and for Gemini worldwide.
****Safeguards* in place for the transfer****	The Firebase Data Processing and Security Terms form part of the agreement with Google (firebase.google.com/terms/data-processing-terms) and do not have to be signed separately. The transfer rests on the EU-US Data Privacy Framework, in which Google participates, and on the Standard Contractual Clauses where that framework does not apply. List of sub-processors: firebase.google.com/terms/subprocessors. For the Gemini API, the terms for paid services apply to customers in the EEA: Google does not use prompts and responses to improve its products (ai.google.dev/gemini-api/terms); the Processing is not tied to a region.
The School gives the Processor written consent for the transfers to third countries or international organisations set out above	□

Transfer 2 — Amazon Web Services (S3 in California, GuardDuty)

Processing (see part D)	3

Description of the transfer outside the EEA	Storage of images, audio fragments and documents uploaded by the teacher, for accounts whose file region is set to the United States. Those files may contain visual material of students or staff and are publicly readable to anyone who has the URL.
Country of Processing or international organisation	United States (California). For accounts on the EU file region the storage remains in Sweden (Stockholm) and there is no transfer.
Safeguards* in place for the transfer	The AWS Data Processing Addendum forms part of the AWS Service Terms automatically (article 1.14) and contains the Standard Contractual Clauses (EU 2021/914); the contracting party is Amazon Web Services EMEA SARL (Luxembourg). AWS also participates in the EU-US Data Privacy Framework. Text: d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.
The School gives the Processor written consent for the transfers set out above	□

Transfer 3 — Vercel Inc. (hosting and running the application)

Processing (see part D)	All
Description of the transfer outside the EEA	Every request to the application and every API call passes through Vercel's servers: students' registration data, answers given, results, uploads and account data. No application data is stored at Vercel (no Vercel database or object storage is in use), but the data is Processed there and appears in the platform's logging.
Country of Processing or international organisation	Germany (Frankfurt) and United States (Washington D.C.) — see G.1. The contracting party is Vercel Inc. (United States); Vercel has no European entity.
Safeguards* in place for the transfer	The Vercel Data Processing Addendum is part of the terms by reference and applies to Pro customers without signature (vercel.com/legal/dpa). It contains the 2021 Standard Contractual Clauses; Vercel also participates in the EU-US Data Privacy Framework. Sub-processors: security.vercel.com.
The School gives the Processor written consent for the transfers set out above	□

Transfer 4 — OpenAI (AI assistant and word check)

Processing (see part D)	17, 18
Description of the transfer outside the EEA	For service 17: the free text the teacher enters, and when translating an activity the full text of that activity. For service 18: the single word a student types in the "wordle" activity type, without a player id and without any further context.
Country of Processing or international organisation	United States.
Safeguards* in place for the transfer	The OpenAI Data Processing Addendum forms part of the agreement (cdn.openai.com/pdf/openai-data-processing-addendum.pdf); the contracting party for the EEA is OpenAI Ireland Limited. The transfer rests on the Standard Contractual Clauses. Data sent through the API is not used to train models unless the customer opts in to that — which has not been done. OpenAI retains logs for abuse monitoring for a maximum of 30 days by default. EU data residency and zero retention require a separate arrangement with OpenAI and have not been arranged. Sub-processors: platform.openai.com/subprocessors.
The School gives the Processor written consent for the transfers set out above	□

Transfer 5 — Twilio SendGrid (email to account holders)

Processing (see part D)	6
Description of the transfer outside the EEA	Name and email address of the account holder and the content of the message. No email is sent to students.
Country of Processing or international organisation	United States.
****Safeguards* in place for the transfer****	The Twilio Data Protection Addendum "forms part of the agreement(s) between Customer and Twilio" (twilio.com/en-us/legal/data-protection-addendum) and contains the Standard Contractual Clauses of 2021/914. For a customer established in the EEA the contracting party is Twilio Ireland Limited (Dublin), according to the table of entities in the Twilio Terms of Service (twilio.com/en-us/legal/tos); Twilio Inc. in the United States is the importer. The transfer rests on the EU-US Data Privacy Framework, Twilio's Binding Corporate Rules and the Standard Contractual Clauses. Sub-processors: twilio.com/legal/sub-processors.
The School gives the Processor written consent for the transfers set out above	☐

Transfer 6 — Stripe (payments)

Processing (see part D)	20
Description of the transfer outside the EEA	Email address and account id of the account holder and the institution's invoicing details. Does not concern Students' data.
Country of Processing or international organisation	Ireland (Stripe Payments Europe, Limited), with transfer to Stripe, LLC in the United States.
****Safeguards* in place for the transfer****	The Stripe Data Processing Agreement itself provides that it "is subject to and forms part of the agreement" (stripe.com/legal/dpa); the Data Transfers Addendum belongs with it (stripe.com/legal/dta). For an account outside North and South America the contracting party is Stripe Payments Europe, Limited (Ireland). The transfer rests on the EU-US Data Privacy Framework and the Standard Contractual Clauses. Sub-processors: stripe.com/legal/service-providers.
The School gives the Processor written consent for the transfers set out above	☐

* Possible safeguards are, for example, an adequacy decision of the European Commission for the country concerned or – in the absence of one, Standard Contractual Clauses (SCC), with, where necessary, sufficient additional measures to safeguard the security of the transfer.

Note, Article 10(1) of the Dutch sector model Data Processing Agreement. The Processor is entitled to transfer outside the EEA only if the School has given **specific written consent** for it. The tick boxes in the tables above are that consent: a School that signs this Schedule with a box ticked has consented to exactly the transfer described there, and to no other.

A School that would rather not give it for a particular transfer can read the tables as a set of choices, because most of these transfers follow from a setting or from an optional service:

- **Transfer 2 (uploaded files) disappears entirely** when the account's file region is set to the EU: the files then stay in Stockholm.
- **Transfer 1 shrinks** when the account's database region is set to the EU. What remains of it is authentication data — Firebase Authentication cannot be set to a region — together with the platform-wide data collections listed in G.1,

and services 13 and 17 if the School switches those on.

- **Transfer 4 (OpenAI) does not arise at all** if the School does not use the AI assistant (service 17) and does not use the "wordle" activity type (service 18). Both are off unless a teacher reaches for them.
- **Transfer 6 (Stripe) does not arise** without a paid subscription, and concerns the School's contract details rather than any Student's data.
- **Transfer 5 (SendGrid)** concerns email to the account holder — a member of staff. The platform sends no email to Students at all.
- **Transfer 3 (Vercel) cannot be switched off**, because it is the hosting on which the application runs. A request from the Netherlands is normally Processed in Frankfurt (see G.1), and no application data is stored at Vercel.

Where a transfer cannot be avoided, the safeguards set out in the tables above apply to it. The Processor is willing to discuss a deviation on any of these points; an agreed deviation is recorded in writing between the parties and takes precedence over this Schedule.

H. Sub-processors

By signing the Data Processing Agreement the School gives the Processor general written consent to engage a Sub-processor. At the time of concluding the Data Processing Agreement the Processor uses the following Sub-processors:

Sub-processor 1

Name of Sub-processor	Google Ireland Limited / Google LLC — Firebase (Realtime Database and Authentication)
Type of Processing	Storage of all account data, activities, results, registrations, class lists and courses in two database instances, and the authentication of teachers and players (including the anonymous sign-in of every player).
(Category of) Personal Data the Sub-processor Processes	All categories from part F: contact details, student number, class, study progress and results, user data, hashed passwords, email addresses, and the free text entered by teachers and students.
Country of storage/Processing of Personal Data by the Sub-processor	Belgium for accounts on the EU region; United States for accounts on the US region and for all platform-wide data collections. Firebase Authentication: managed by Google, not regionally configurable.
Country of establishment of the Sub-processor	Ireland (Google Ireland Limited) / United States (Google LLC). See part G, transfer 1.

Sub-processor 2

Name of Sub-processor	Amazon Web Services, Inc. / Amazon Web Services EMEA SARL — Amazon S3 and GuardDuty Malware Protection
Type of Processing	Storage of images, audio fragments and documents uploaded by teachers, and the malware check on uploaded documents before publication.
(Category of) Personal Data the Sub-processor Processes	Image and audio material and documents which may contain personal data (including visual material of Students and staff), with the teacher's account id in the file key.
Country of storage/Processing of Personal Data by the Sub-processor	Sweden (Stockholm) for accounts on the EU file region; United States (California) for accounts on the US file region.

Country of establishment of the Sub-processor	United States / Luxembourg. See part G, transfer 2.

Sub-processor 3

Name of Sub-processor	Vercel Inc.
Type of Processing	Hosting, delivery and running of the web application and of all API endpoints, including the scheduled tasks. All data traffic between the browser and the storage passes through this party.
(Category of) Personal Data the Sub-processor Processes	All categories from part F, in transit; in addition connection data including the visitor's IP address. No application data is stored at this Sub-processor.
Country of storage/Processing of Personal Data by the Sub-processor	Germany (Frankfurt) and United States (Washington D.C.); a request goes to the nearest region. See part G.
Country of establishment of the Sub-processor	United States. See part G, transfer 3.

Sub-processor 4

Name of Sub-processor	OpenAI Ireland Limited (contracting party for customers in the EEA); the Processing takes place at OpenAI, L.L.C. in the United States
Type of Processing	Generating content at a teacher's request (service 17) and checking whether a word typed in by a student exists (service 18).
(Category of) Personal Data the Sub-processor Processes	For service 17: the free text the teacher enters, including the full text of an activity in a translation job — that text may contain personal data if the teacher has put it there. For service 18: one word typed in by a student, without identifying data.
Country of storage/Processing of Personal Data by the Sub-processor	United States.
Country of establishment of the Sub-processor	United States. See part G, transfer 4.

Sub-processor 5

Name of Sub-processor	Google Ireland Limited / Google LLC — Gemini (Generative Language API)
Type of Processing	Converting an uploaded document, worksheet or photograph into exercises, and generating and editing images, at a teacher's request (service 17).
(Category of) Personal Data the Sub-processor Processes	The full content of the file or image uploaded by the teacher, including any personal data in it, and the description entered.
Country of storage/Processing of Personal Data by the Sub-processor	Worldwide; no region can be set on the API used.
Country of establishment of the Sub-processor	Ireland / United States. See part G, transfer 1.

Sub-processor 6

Name of Sub-processor	Twilio Inc. — SendGrid
Type of Processing	Sending email to the account holder about the account, the subscription, invitations, limits and platform messages. No email is sent to Students.
(Category of) Personal Data the Sub-processor Processes	Name and email address of the member of staff of the School, and the content of the message.
Country of storage/Processing of Personal Data by the Sub-processor	United States.
Country of establishment of the Sub-processor	United States. See part G, transfer 5.

Sub-processor 7

Name of Sub-processor	Stripe Payments Europe, Limited (contracting party); transfer to Stripe, LLC
Type of Processing	Handling payments, subscriptions and invoicing for a paid subscription. Payment card details are entered and Processed solely at Stripe.
(Category of) Personal Data the Sub-processor Processes	Email address and account id of the account holder, the institution's invoicing details, and the payment details the payer enters at Stripe. No data of Students.
Country of storage/Processing of Personal Data by the Sub-processor	Ireland and United States
Country of establishment of the Sub-processor	Ireland. See part G, transfer 6.

Sub-processor 8

Name of Sub-processor	Pixabay GmbH
Type of Processing	Searching a stock photograph library at a teacher's request. The search request is sent from the server; the user's browser does not connect to Pixabay, and a chosen photograph is copied to Puzzel.org's own storage.
(Category of) Personal Data the Sub-processor Processes	Solely the search term the teacher types in. No account id, IP address or other identifying data is sent along.
Country of storage/Processing of Personal Data by the Sub-processor	Germany.
Country of establishment of the Sub-processor	Germany.

Other recipients — not Sub-processors

The following parties receive personal data, but not as a Sub-processor of Puzzel.org. They are listed here because the School must be able to weigh them up.

Party	Role and data received
Google Classroom, within the school's Workspace domain	The school is itself the controller for its Classroom environment. On the teacher's instruction Puzzel.org sends only the grade achieved there, to a submission that already exists in that teacher's class.
The school's learning environment (LTI 1.3)	Likewise: the school hosts and manages the platform itself; Puzzel.org sends only the grade achieved there and receives the identity data the school itself shares.
Video and documents embedded by the teacher	If a teacher places a YouTube or Vimeo video or a Google Drive or OneDrive document in a course, the student's browser connects to that party. Only privacy-friendly variants are permitted (YouTube in cookie-free mode, Vimeo with tracking switched off); arbitrary embeds are refused.

After the Data Processing Agreement has been concluded, the Processor has the right to use Sub-processors other than those listed in these Details of Processing, provided that notice of this is given to the School in advance and that the School can object to it within six weeks (Article 11(2) of the Dutch sector model Data Processing Agreement).

Schedule 1 (Details of Processing) forms part of the arrangements made in the Convenant Digitale Onderwijsmiddelen en Privacy 4.0, the Dutch sector agreement on digital educational resources and privacy, an initiative of the PO-Raad, VO-raad, MBO Raad, the various sector parties involved (MEVW, KBb-E and VDOD) and the Dutch Ministry of Education, Culture and Science. More information can be found at www.privacyconvenant.nl.

SCHEDULE 2: SECURITY MEASURES — Puzzel.org

Processor: **Puzzel.org**. Version **1.0**, date of last amendment **20 September 2026**.

Under the GDPR and clause 5 of the Data Processing Agreement, the Processor is obliged to take appropriate technical and organisational measures to secure the Processing of Personal Data, and to demonstrate those measures. This Schedule gives a concise description and enumeration of those measures.

The assessment in Part B is made against the 'Certification Scheme for Information Security and Privacy ROSA' (*Certificeringsschema informatiebeveiliging en privacy ROSA*), the certification scheme of the Dutch education sector, published by Edustandaard at www.edustandaard.nl. A School outside the Netherlands will not know this scheme; it is named here so that it is clear that the Processor has assessed itself against a recognised sector framework rather than against none.

Some of the measures the model lists as a matter of course assume an organisation with several employees and an established administrative process. Puzzel.org is a one-person business. Where a measure does not in fact exist, this Schedule states that as "Not met", with the reason, instead of a reassuring formulation. The Processor regards an honest security annex with open points as a smaller risk for the School than a flattering one.

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

1. The Processor has an appropriate policy for the security of the Processing of Personal Data, which policy is evaluated periodically and – where necessary – amended.

The policy is set out in a short document, *Information Security Policy Puzzel.org*, adopted on **20 September 2026**. It is evaluated annually, at the same time as the self-assessment under Part B and after every incident of significance.

What in fact does exist, and can serve as the basis for that policy:

- Access to data is enforced by the database access rules, which are applied on Google's servers and not in the browser. The database is closed by default: there is no general read or write permission at the top level, so that every data node that has not been expressly opened up is closed.
- In September 2026 two independent security investigations were carried out (see Part B, "Form of assessment") and their findings have largely been dealt with.
- Changes to the access rules are tracked in a change log kept with those rules themselves.

2. The Processor takes measures so that, through a system of authorisation, only authorised employees can gain access to the Processing of Personal Data under the Data Processing Agreement. Under this system, employees do not have access to more data than is strictly necessary for their role.

- **Puzzel.org has one employee**, who is also the owner. There is no second person to whom rights have been granted, and therefore no separation of duties. This is the factual situation. If a second person ever joins, that person will be given only the rights needed for the task, and this Schedule will be amended accordingly.
- **For the user, authorisation is systematic.** Every read and write operation passes through the database access rules. An account reaches only its own data and the results submitted on its own activities. A Student can read only their own result: for this the rules test whether the signed-in account is the player themselves. A teacher connected to a school account is given access to that school's shared library, and only under a condition tied to the identification of that school.
- **Administrator access** (the "puzzle master" console, 52 endpoints) requires a server-verified login token *and* an administrator record in the database. That record can be written only by server code and is unwritable for every

user, so that nobody can make themselves an administrator.

- **Access to a customer account for support.** There is a function with which the administrator can sign in as a user. That function is secured with the same administrator check and has **no second factor and no reason field**. Every use is recorded, however: which administrator, which account and when, with internal account numbers and without an email address. That recording takes place *before* access is granted; if it fails, access is refused. That the function is used only at the express request of the account holder, and only to investigate a reported problem, is a working arrangement and not a technical measure; the published supplier information states the same.

3. The Processor has an information security coordinator to identify risks around the processing of Personal Data, to promote security awareness, to check facilities and to take measures directed at compliance with the information security policy.

This role is fulfilled by the owner, who is also the only employee. There is no independent coordinator. This is the factual situation. There is no independent supervision within the organisation; the investigations under Part B are the means by which the self-assessment is tested.

4. Information security incidents are documented and are used to improve the information security policy.

An incident register is kept: for each incident the date of discovery, the nature, the data and Data Subjects affected, the measures taken and the date of closure.

5. The Processor has a process in place for communication about information security incidents.

See Part C. Notification is made by email to the account holder, by the contact person named in Part C. The School is informed without delay, and at the latest within 48 hours of discovery.

6. The Processor concludes confidentiality undertakings with employees and makes information security arrangements.

Not applicable: there are no employees besides the owner. The owner's duty of confidentiality follows from clause 4 of the Data Processing Agreement itself. Any future employee or contractor signs a confidentiality undertaking in advance.

7. The Processor promotes awareness, education and training in respect of information security.

There is no formal training programme; the organisation consists of one person. The owner carries out the self-assessment under Part B annually, acts on the security advisories for the software dependencies used, and has the software investigated for security periodically.

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

Set out below is the report of the BIV classification, the degree of compliance and the explanation of any deviations from the standards. For this the Processor uses in principle the 'Certification Scheme for Information Security and Privacy ROSA' (*Certificeringsschema informatiebeveiliging en privacy ROSA*, to be found at www.edustandaard.nl) as its assessment framework and to create a sound baseline level of information security and privacy. BIV is the Dutch scheme's abbreviation for Availability, Integrity and Confidentiality.

Form of assessment	**Self-assessment (level 1).** The declaration is given by the owner himself. Carried out on **20 September 2026**, on the basis of the Certification Scheme assessment framework **v4.0** (Edustandaard, December 2025).
Assessment carried out by	Puzzel.org — Daan Weustenraad, owner
Login page	https://puzzel.org/en/auth

BIV classification	**Availability = M (Medium)**, **Integrity = M (Medium)**, **Confidentiality = M (Medium)**, established according to the classification questions of the Certification Scheme assessment framework v4.0 (Edustandaard, December 2025), in which for each aspect the highest answer counts. _Reasoning:_ the product is practice and assessment material, not a student administration system or student tracking system and not an examination system; an outage does not affect any statutory record, but the service is also used in the evenings and at weekends, an outage lasting days is not acceptable, and an outage hinders a lesson that could otherwise go ahead (A = medium). The results are used by teachers to assess progress and can be written to a gradebook as a grade, which means that inaccuracy has consequences (I = medium). No special categories of personal data and no citizen service number (BSN) are processed, but names, email addresses, student numbers and learning results of minors are (C = medium). **A school that deploys the product for assessment with consequences must judge for itself whether I and C come out higher for it.**

Category	Measures	Compliance	Explanation
Availability	Design	Met	Redundancy is provided by Vercel and Google, and an external availability check gives notice of an outage (see the "Monitoring" row). The application runs serverless at Vercel and the data is held in Google Firebase Realtime Database; both are managed, redundantly operated services. There is no server or network equipment of the Processor's own. The play page reads the content directly from the database and is therefore not dependent on the availability of the Processor's own server functions.
	Capacity management	Not met	**Deviation (Medium level):** there is no trend analysis and no active alerting against a pre-set threshold; scaling is left entirely to Vercel and Google. Scaling is managed by Vercel and Google. At application level there are rate limiters on approximately 25 public endpoints and a limit of 10 calls per day per key on the public API.
	Maintenance	Not met	**Deviation (Medium level):** maintenance does not take place to a plan, and one software dependency has deliberately not yet been updated while a security advisory for it remains open. A rollback scenario does exist: Vercel can restore any earlier deployment immediately. Maintenance is carried out by the owner; there is no maintenance window and no agreed service window. No availability commitment or SLA is offered: the service is provided on a best-efforts basis, with support by email between 09:00 and 22:00 CET.
	Testing	Not met	**Deviation (Medium level):** there is no availability regression test after a release, no annual load test and no automated build pipeline; tests and the type check are started by hand. There is an automated type check across the entire software and there are unit tests, including a test suite against the database access rules on a local emulator. There is **no** acceptance environment with real data; changes are tried out on a Vercel preview and locally.
	Monitoring	Met	An external availability check (UptimeRobot) checks the website and a server route every five minutes, each time on the content of the response and not only on the status code, and alerts the owner by email in the event of an outage. The service retains three months of availability history, which a School can obtain on request. There is no separate error-monitoring service: errors in the application itself are noticed by the owner or through a report from a user.

Category	Measures	Compliance	Explanation
	Recovery	Not met	**Deviation (Medium level):** the standard requires a periodic recovery test; that does not take place. This is a deliberately accepted risk. Recovery of the database is possible from the daily backup of Firebase (see the "Backup" row). The recovery process has not been tested, and for uploaded files there is no means of recovery.
Integrity	Traceability (users)	Not met	**Deviation:** changes cannot be rolled back individually (there is no version history, only the daily backup) and changes to data cannot be inspected after the fact. The timestamps on a result are set by the player's browser, not by the server. Every write operation is bound to a verified user: the access rules test which account is signed in, and every server call verifies the login token. For a result it is checked that it is written under the player's own record, so that a player cannot write a row under someone else's name. Grades are calculated on the server from the answers given and are never taken over from the browser.
	Backup	Not met	**Deviation:** the daily frequency is achieved, but the integrity of the backup is not checked quarterly, there is no separation of duties (one person) and uploaded files have no backup (a deliberately accepted risk, see below). For both instances of the Firebase Realtime Database (US and EU), the **daily automatic backups** of Firebase are switched on; a backup is retained for 30 days. For the uploaded files in Amazon S3, **no versioning and no backup** has been set up: a deleted or overwritten file cannot be retrieved. This is a deliberately accepted risk: these are images, audio and documents attached to activities, which the teacher can upload again; results and registrations of Students are held in the database and are covered by the daily backup. Amazon S3 itself keeps every file redundantly in several locations, so that equipment failure does not lead to loss. There is no tested recovery procedure.
	Application controls	Alternative measure	**Alternative measure:** the play data deliberately goes straight from the browser to the database, so that changes do not pass through an application layer of the Processor's own; the database access rules, which are applied on Google's servers, perform that controlling role. Input is validated both in those rules and on the server: length limits and permitted fields on submitted data (for example a leaderboard row with seven permitted fields and a label of at most 500 characters), a strict pattern on the word check, and type detection on uploaded files based on the content of the file instead of what the browser reports. Outgoing HTML in email is sanitised.
	Non-repudiation (data)	Not met	**Deviation:** the standard requires functional logging of changes to (personal) data, retained for 13 months. No such change log exists. For a result it is recorded who the player is, whose the activity is, when it was created and when it was last played. A changed grade in the gradebook is visible to the school.
	Traceability (technical administration)	Not met	All changes to the software are held in a version control system with author and timestamp. Changes to the database access rules are pasted **by hand** into Google's two management consoles; there is one recorded reference version of those rules, but it is not the source of truth. This is a deliberately accepted risk of divergence between the two regions; after every change the rules in both consoles are compared against the reference version. Administrator access to a customer account is recorded (see A.2).

Category	Measures	Compliance	Explanation
	Integrity checking	Not met	**Deviation:** the malware check applies only to documents in the course section; images and audio are not checked. There is no recorded guideline for secure programming and no structural checking of the configuration. Uploaded documents are checked for malware in quarantine before they can be published, and are published by way of a copy within the storage service, so that the published file is exactly the file that was checked. File types are derived from the content of the file.
	Non-repudiation (application)	Not met	**Deviation:** the standard requires technical logging of administrator activity and of changes to configuration and application, with a monthly review. Every time the owner signs in as an account holder this is recorded (who, which account, when); other administrative actions and configuration changes are not logged, and there is no monthly review. Messages to a school's learning environment are signed with a key that exists only in the running environment and whose public half is published at a fixed address; incoming messages are checked against the public keys of the school's platform. The state value passed when linking to a gradebook is signed and valid for at most 30 minutes.
Confidentiality	Data lifecycle	Not met	**Deviation:** there is no automatic retention period; data remains in place until the teacher or the School deletes it. See Part F.2 of Schedule 1. Deletion of an account erases all data linked to the account in **both** regions, removes the files from object storage, revokes the Google Classroom token at Google and deletes the login. **Not erased** are a few platform-wide records (the send record for email, the payment administration, submitted feedback). There is **no** automatic expiry period for results and registrations.
	Logical access	Not met	**Deviation:** the standard requires two-factor authentication, enforced by default for every user who sees other people's data, and password requirements in line with NIST. The application offers no two-factor authentication of its own; a teacher who signs in with Google or Microsoft inherits that of the provider, a teacher with an email address and password does not. The minimum for a password is eight characters, enforced by Firebase Authentication; the sign-up page and the change-password screen state that same minimum. Access itself is enforced by the access rules on Google's servers; see A.2. One particular point must be mentioned here: the answers to an activity are held in a separate part of the database that is readable only by the owner, because the play page reads the content directly from the database. The conversion happens when an activity is (re-)saved; **older activities that have not been saved again still carry their answers in the publicly readable content part.**
	Physical access	Met	There is no data centre of the Processor's own and no equipment of its own. Physical security rests with Google, Amazon Web Services and Vercel; see Part H of Schedule 1.
	Network access	Alternative measure	**Alternative measure:** there is no network of the Processor's own and therefore no network zones or jump server. Administration runs exclusively through the management consoles of Google, Amazon Web Services and Vercel, all three of which are secured with two-factor authentication. All traffic runs over HTTPS. There is no network of the Processor's own and no VPN. The connection to the database runs over an encrypted connection. Access to the administration environment requires the same verified token as above.

Category	Measures	Compliance	Explanation
	Separation of environments	Not met	There is no separate acceptance or test database: both databases are production and no staging copy exists. A standing working instruction applies that no test data is written to the production databases; for end-to-end checks one test account has been designated. Changes are tried out locally and on a Vercel preview.
	Transport and physical storage	Met	**Measured.** Conformity with the Uniform Security Requirements for TLS (*Uniforme Beveiligingsvoorschriften TLS*) of Edustandaard was measured with internet.nl on 20 September 2026; the HTTPS section ("Connection sufficiently secured") is entirely green, as are DNSSEC and RPKI. Encrypted transport (HTTPS/TLS) to all services, with HSTS for a year including subdomains and inclusion in the preload list of the browsers, and with enforcement of an encrypted connection. No physical transport or physical storage of data carriers takes place.
	Logging	Not met	**Deviation:** the standard requires logging of successful and failed access and of the reading of personal data; neither of the two exists. **No** request log is kept in the application; there is no log line that writes an IP address or an email address. The few server lines that can touch a person name an internal account number or a hashed value. The underlying logging of the hosting party falls outside the application. The other side of this is that there is no access log with which to reconstruct an incident; in the event of an incident only the standard logging of Vercel is available, which is retained briefly. At the chosen classification (C = medium) this is a recognised deviation.
	Vulnerability management	Not met	**Deviation:** three findings from the investigation of 13 September 2026 are still open: activities with an access restriction are readable outside the browser; the decoding of very large images is not yet bounded (the remaining part of that finding has been closed); and one software dependency has deliberately not yet been updated while a security advisory for it remains open. Conformity with the Uniform Security Requirements for TLS of Edustandaard, to which this standard refers, was measured on 20 September 2026 and found to be in order (see the "Transport and physical storage" row). Software dependencies are tracked and security notices are acted on; a number of components have deliberately been fixed to a particular version because a newer version fails in production, and the reasons for this are recorded. In September 2026 two independent investigations were carried out (see below), the findings of which have largely been dealt with. Vulnerabilities are resolved according to severity: **critical within 2 days, high within 30 days** of being established. Vulnerabilities can be reported via daan@puzzel.org.

Investigations carried out

Two investigations were carried out in September 2026 and recorded in writing. Both are **investigations of the software and the configuration, supported by tests on a local database emulator — not a penetration test of the running service.**

1. **Security investigation of 13 September 2026.** Scope: 139 endpoints, of which 49 administrator endpoints, the shared authentication, the database access rules, the billing and webhooks, the storage, player registration and results, the permissions around school accounts and the library, and a search for secrets in the software. Thirteen findings: one critical (provided the key remained active), seven high, five medium.
2. **Investigation of the difference between the software and the access rules, of 13 September 2026.** Approximately 35 findings on the seam between what the software does and what the access rules allow, each tested by a second reviewer and recalculated on the emulator.

Status. Of the thirteen findings from the security investigation, ten have been closed, including the critical finding (a key for server access, revoked and verified) and the finding from the second investigation about multiplayer sessions; the corresponding rules are in place in both management consoles. **Three findings are open.**

- Activities with an access restriction are readable outside the browser. This finding has not yet been resolved; a worked-out plan is in place.
- The finding about the load on the server from uploads has largely been closed: the uploading of images and the measurement for spot-the-difference have a limit per user and per address. What remains open is that a very large image is fully decoded before its dimensions are known.
- One software dependency has not yet been updated to the version in which the open security advisory is remedied.

The rules in both management consoles are identical to the recorded reference version.

Measures found at application level

- A closed database as the starting point; not a single publicly writable path. The top level of the access rules itself has no read or write permission and no wildcard, so that every data node without a rule of its own is closed. Nine data nodes in use therefore have **no rule of their own** — among them the record of administrator access, the payment administration and the processing of payment notifications. All nine are read and written exclusively by server code, with administrator rights that bypass the rules in any case; for the browser they are closed.
- Results shielded per player: a player reads only their own row.
- Answers to activities in a separate part of the database that is readable only by the owner.
- The leaderboard as a shielded view with masked email addresses and telephone numbers.
- Administrator endpoints solely on a verified login token plus an administrator record written by the server.
- Security headers on every response: HSTS (1 year, including subdomains, with inclusion in the preload list), the prohibition on guessing the file type, a restricted referrer, and a prohibition on embedding by other websites except on the routes that are expressly embeddable.
- Protection against form submission from another website, with an express list of permitted paths for the link to a learning environment.
- Rate limiting on approximately 25 public endpoints, with measures against concurrency, and with salted hashed addresses instead of IP addresses.
- Malware checking of uploaded documents before publication, with structural sanitisation of PDFs.
- The refresh token for Google Classroom stored encrypted (AES-256-GCM) with a separate key that exists only in the running environment.
- Passwords of courses and of class members hashed with scrypt and a salt of their own, compared in constant time.
- Identities from a school's learning environment stored as hashed values; log lines never show the raw identity.
- All secrets out of the settings of the running environment; no fallback to a file, no secret in version control.
- Re-confirmation of the password before deletion of the account and before a change of region.
- Scheduled tasks secured with a secret, compared in constant time, failing when a value is missing.

Points a School must expressly weigh

The model asks for a concise but honest enumeration. The following points belong in it.

1. **Uploaded images, audio and documents are publicly readable.** They are given a public URL in the object storage; whoever has the URL can retrieve the file. There is no access control on these files. The published supplier information says this too: treat material in activities as public and put nothing confidential in it.

2. **A number of data nodes are deliberately publicly readable**, because the play page reads the content directly from the database and not by way of a server. This concerns the content of an activity (per activity, not per teacher), the subscription level of the owner, the styling preferences, the multiplayer sessions, and — for Puzzel LMS — the **display names on the class list**. Full names, email addresses and password hashes of class members are held in a shielded part that only the teacher reads. Also world-readable are the teacher → school link and an individual invitation to a school account (with the name and email address of sender and recipient) for anyone who knows the key of that invitation.
3. **There is no general Content-Security-Policy**, that is to say: no rule that lays down which scripts and which sources a page may load. Only the prohibition on embedding by other websites and the enforcement of an encrypted connection are present. The measurement with internet.nl of 20 September 2026 comes out at 86% partly for this reason: the HTTPS section is entirely green, but under "Security options" the Content-Security-Policy is missing, and the domain is not reachable over IPv6. Neither of the two touches the encryption of the traffic; both are stated here because a school can run the same test.
4. **There is no two-factor authentication** in the application itself; a teacher who signs in with Google or Microsoft inherits that of the provider. A password counts at least eight characters: that minimum is set as the password policy in Firebase Authentication, and the sign-up page and the change-password screen state it as well.
5. **The access rules are placed by hand in two management consoles.** There is one recorded reference version of those rules; whether both regions are running exactly these rules is a matter of discipline and has to be checked.
6. **The backup regime is limited**: daily backups of the database, no backup of uploaded files and no tested recovery procedure (see the "Backup" row above).
7. **Uploaded photographs are not stripped of metadata.** There is nothing in the application that removes EXIF data — including location data — from an uploaded photograph. A photograph of a school playground or a class can therefore carry location data in a publicly retrievable file. This is the factual situation at present.
8. **There is no automated build pipeline.** There are unit tests — including a test suite against the database access rules on a local emulator — and a type check across the entire software, but nothing runs them of its own accord: there is no environment that runs the tests automatically, no command that runs all the tests one after another, and no working automatic check when a change is committed (the files present for that purpose are remnants of a removed utility and do nothing). Every test and the type check are started by hand, so that a change can be deployed without a test having been run. See also the "Testing" and "Integrity checking" rows above.
9. **The timestamps on a result are set by the player's browser**, not by the server. The time of creation and the time of last play are set on the play page from the clock of the device and written to the database that way; the access rules test only *that* it is a number, not whether it is anywhere near the time of the server. Everything that is security- or billing-relevant does run on the clock of the server. This is not a leak, but a school that uses results as evidence that work was done at a particular moment must know that that moment has not been established independently.

Instead of the 'Certification Scheme for Information Security and Privacy ROSA', the Processor may also make use of other certification mechanisms and/or (inter)nationally recognised norms and standards for information security, provided that these offer an equivalent or higher level of security and that the measures taken by the Processor are made transparent to the School.

C. Arrangements on informing about security incidents and/or Personal Data Breaches

The Processor has a procedure for the monitoring and identification of incidents and for informing in the event of Personal Data Breaches and/or incidents relating to security. In such a case the Processor will provide the Controller with the following information:

- the characteristics of the breach, such as: date and time of discovery and duration of the breach; a summary of the breach, including the nature of the breach and the nature and description of the security incident (which part of the

security it relates to, how it occurred, whether it relates to reading, copying, altering, deletion/destruction and/or theft of Personal Data);

- the cause of the breach;
- how the breach was discovered;
- the measures taken to address the breach and to prevent any (further and future) damage;
- whether the Personal Data involved in the breach were encrypted, hashed, etc.;
- the group(s) of Data Subjects who may experience consequences from the incident, and the numbers and size of the group(s) of Data Subjects;
- what the possible consequences of the breach are for the School and the group(s) of Data Subject(s), including where possible an assessment of the risk of the consequences for the group(s) of Data Subject(s);
- the quantity and type of Personal Data involved in the breach (in particular special categories of Personal Data such as data on health or religion, or data of a sensitive nature, including access or identification data, financial data or learning performance).

In the event of a (suspected) security incident and/or Personal Data Breach, the School and the Processor may in principle contact each other by email via the contact details below.

	Name and role of contact person for security incidents/Personal Data Breaches	**Contact details (email and telephone number)**
Processor	Daan Weustenraad, owner. There is no second contact person and no escalation path; the published supplier information also states this expressly. There is no stand-in during absence.	daan@puzzel.org No telephone number is published; notifications are made by email.
The School	[To be completed by the School]	[Idem]

Notification period. The School is informed without delay, and at the latest within 48 hours of discovery of the breach, so that it can report a notifiable personal data breach to its own supervisory authority within the 72 hours that Article 33(1) GDPR allows.

Detection. There is no active monitoring, no alerting and no access log. In practice an incident is noticed by the owner during day-to-day administration, through a report from a user or a School, or through a report from a Sub-processor.

Schedule 2 (Security Measures) forms part of the arrangements made in the Convenant Digitale Onderwijsmiddelen en Privacy 4.0 (the Digital Educational Resources and Privacy Covenant 4.0), a Dutch education-sector agreement, an initiative of the PO-Raad, VO-raad, MBO Raad, the various supply-chain parties involved (MEVW, KBb-E and VDOD) and the Ministry of Education, Culture and Science. Further information on this can be found at www.privacyconvenant.nl.