

Data Processing Agreement

under Article 28 of the General Data Protection Regulation (GDPR)

Document version: 2026-09-04

Effective date: September 4, 2026

Controlling language: German

This Agreement follows the structure of the standard contractual clauses between controllers and processors under Commission Implementing Decision (EU) 2021/915. Its annexes form part of the Agreement. The German version controls; this translation is provided for understanding.

Parties

Controller

Legal name of the school, school authority, educational institution, or teacher acting as controller in their own right:

Address:

Represented by, role:

Privacy contact or data protection officer:

referred to as the "Controller".

Processor

Intelligrade UG (haftungsbeschränkt)

Bebelallee 123, 22297 Hamburg, Germany

Represented by managing director Kevin Peters

Email: kevin@intelligrade.de

referred to as "Intelligrade" or the "Processor".

1. Subject matter, precedence, and scope

1. This Agreement governs Intelligrade's processing of personal data on the Controller's behalf when the Controller uses the Intelligrade platform. Annex 1 describes the subject matter, nature, purpose, and scope.
2. The main agreement includes the Terms of Service and agreed service features. This Agreement prevails where terms conflict on commissioned processing. Mandatory data protection law prevails over both.
3. The Controller is normally the school, school authority, or other competent educational institution. A teacher is the Controller only when the teacher lawfully determines the purposes and means in their own responsibility.
4. Intelligrade acts as Processor for classroom, exam, and result data. Intelligrade acts as an independent controller for teacher registration and account management, account security, billing, fraud prevention, and direct support administration. The Privacy Policy, rather than this Agreement, governs those independent purposes.

2. Duration

1. This Agreement applies from electronic conclusion or signature and remains in effect while Intelligrade processes personal data on the Controller's behalf.
2. It ends with the main agreement after Intelligrade returns or erases commissioned data under Section 11. Confidentiality, evidence, and legally required retention duties survive.

3. Instructions and responsibility

1. Intelligrade processes commissioned data only on the Controller's documented instructions. This Agreement, the main agreement, settings used in the platform, and instructions in text form are documented instructions.
2. If Union or Member State law requires further processing, Intelligrade will inform the Controller before processing unless that law prohibits notice on important grounds of public interest.
3. If Intelligrade considers an instruction unlawful, it will inform the Controller without undue delay and may suspend the instruction until the Controller confirms, changes, or withdraws it.
4. The Controller decides the purposes, means, legal bases, notices, retention periods, and permissibility of use in its school context. It will issue lawful instructions and keep its contact details current.
5. Special categories under Article 9 GDPR and data about criminal convictions or offences under Article 10 GDPR are not an intended product feature. They may nevertheless appear in free text, materials, or feedback. The Controller will instruct users to enter such data only with a valid legal basis. Intelligrade applies the safeguards in Annex 2.

4. Intelligrade's obligations

Intelligrade will

- process commissioned data only for agreed purposes and on documented instructions;
- limit access to people who need it for their work and are bound by contractual or statutory confidentiality;
- maintain the measures in Annex 2 and develop them in line with risk and the state of the art;
- provide information needed to demonstrate compliance with Article 28 GDPR;
- forward data-subject requests to the Controller without undue delay instead of responding on substance, unless the law requires a response;
- not sell personal data, use it for advertising, or use it to train its own AI models;
- inform the Controller without undue delay of an instruction, request, or official order concerning commissioned data, where legally permitted.

5. Security of processing

1. Intelligrade implements measures appropriate to the risk under Article 32 GDPR, taking account of the state of the art, implementation costs, and the nature, scope, context, and purposes of processing. Annex 2 lists the agreed current measures.
2. Intelligrade may change a measure if the agreed protection level does not decrease. Intelligrade documents material changes.
3. The Controller will manage roles, sharing, and student and parent access codes carefully. It will revoke access that is no longer required and give codes only to their intended recipients.

6. Personal data breaches

1. Intelligrade will notify the Controller of a breach affecting commissioned data without undue delay after becoming aware of it.
2. As information becomes available, the notice will describe the nature and scope of the breach, categories and approximate numbers of affected people and records, likely consequences, measures taken or proposed, and a contact

point. Intelligrade will provide missing facts in later notices without undue delay.

3. Intelligrade will document the incident, preserve evidence, limit its effects, and assist the Controller with notifications under Articles 33 and 34 GDPR. The Controller decides whether to notify authorities and data subjects unless the law provides otherwise.

7. Assistance to the Controller

Taking account of the nature of processing and information available, Intelligrade will assist with

- access, rectification, erasure, restriction, portability, and objection requests;
- processing security and restoration after incidents;
- data protection impact assessments and prior consultations under Articles 35 and 36 GDPR;
- information, evidence, and notification duties;
- return, export, and erasure of commissioned data.

The platform provides a machine-readable export of structured commissioned data and a file manifest with time-limited download links. If the Controller needs other assistance, the parties will agree its scope and a secure transmission method.

8. Sub-processors

1. The Controller gives Intelligrade general authorization to use the sub-processors listed in Annex 3.
2. Intelligrade will give at least 14 calendar days' notice before adding or replacing a sub-processor. The notice will identify the provider, location, task, and intended safeguards.
3. The Controller may object within that period for specific data protection reasons. The parties will seek a reasonable solution. If none is possible, the Controller may disable the affected feature or terminate the main agreement for the affected processing.
4. Intelligrade will impose data protection obligations at least equivalent to this Agreement, remains responsible to the Controller for sub-processor performance, and will provide the essential contractual terms on request. Trade secrets and confidential details may be redacted.

9. Processing locations and international transfers

1. The main infrastructure and AI processing listed in Annex 3 are in Germany or the European Union.
2. A transfer to a third country will occur only on documented instruction or under a mechanism in Chapter V GDPR. Intelligrade will identify the mechanism and add appropriate safeguards and supplementary measures where needed.
3. A data subject's access from a third country does not by itself constitute a transfer by Intelligrade to a recipient in that country.

10. Evidence and audits

1. On request, Intelligrade will provide suitable evidence such as current security descriptions, audit reports, certificates, or answers to a reasonable questionnaire.
2. Where that evidence is sufficient, document-based and remote audits take priority. Where justified, the Controller or an independent auditor bound by confidentiality may conduct an on-site audit.
3. Audits require reasonable notice, take place during normal business hours, and remain limited to commissioned processing. They must not compromise security, other customers' rights, or trade secrets. A shorter notice period may apply after a security incident or official order.
4. Intelligrade will cooperate with the competent supervisory authority and permit its statutory powers.

11. Return, erasure, and termination

1. At the end of the services or on a lawful instruction, Intelligrade will return or erase commissioned data at the Controller's choice unless Union or Member State law requires retention.
2. Intelligrade will erase data from active systems within 30 days, including related exam files. Backups expire through the normal backup cycle no later than 90 days and are not processed for another purpose during that period.
3. Intelligrade will restrict legally retained data to the required purpose and erase it when the retention period ends. It will confirm erasure on request.
4. The Controller should retrieve its export before termination. It must download files before their time-limited links expire.

12. Protestant and Catholic data protection law

1. If the Controller is subject to the Data Protection Act of the Evangelical Church in Germany, this Agreement also constitutes a commissioned-processing agreement under Section 30 DSG-EKD in its applicable version. Statutory information, inspection, and supervisory powers remain unaffected.
2. If the Controller is subject to the Catholic Church Data Protection Act, this Agreement also constitutes a commissioned-processing agreement under Section 29 KDG in its applicable version. Statutory powers of the Catholic data protection authority remain unaffected.
3. The parties will additionally apply any mandatory church-law requirements. Before processing begins, the Controller will tell Intelligrade which law and supervisory authority apply.

13. Final terms

1. Amendments require text form unless mandatory law requires stricter form.
2. If a provision is invalid, the remaining provisions remain effective. The parties will replace it with a valid provision closest to its lawful purpose.
3. German law applies. Mandatory jurisdiction and procedural rules, including rules for public bodies and supervisory authorities, remain unaffected.
4. The German version is the binding contract. Translations are provided for understanding.
5. The parties may conclude the Agreement in writing or electronically. For electronic conclusion, Intelligrade records the Controller and representative identity, confirmed authority, document version, document checksum, language, and conclusion time.

Annex 1: Description of processing

Item	Agreed description
Subject and purpose	A platform to create classrooms and exams, conduct exams, collect answers, grade automatically and manually, provide feedback, show results, and optionally record parent or guardian confirmation.
Operations	Collection, recording, organization, storage, retrieval, display, alteration, matching, disclosure to approved sub-processors, restriction, export, and erasure.
Data subjects	Students, parents and guardians, teachers, and other school staff where their data is processed on instruction.
Master data	Names or pseudonyms, classroom and subject assignments, internal identifiers, roles, and sharing permissions.
Access and usage data	Generated student and parent access codes, session identifiers, sign-in and submission timestamps, IP address, and browser details in time-limited security logs.
Exam and content data	Questions, materials, images, answers, markings, progress, comments, corrections, feedback, points, grades, and grading scales.
Result and confirmation data	Exam status, results, student comments, and the time of parent confirmation. Intelligrade does not create a parent identity record.
Special data	Not intended. It may appear incidentally in free text or materials.
AI processing	When AI grading is enabled, the free-text answer, question title, description or material, marking expectations, points, and a short language sample go to Mistral AI. Structured student names are not sent. Free text may contain identifiers. The teacher reviews the suggested output.
Duration	Term of the main agreement plus the return and erasure period in Section 11.
Frequency	Continuous while the platform is used. AI processing occurs only when the feature is enabled.
Locations	Primarily Germany. Optional AI processing uses Mistral AI's EU endpoint.

Annex 2: Technical and organizational measures

1. Organization and access

- Individual privileged administrator accounts, multi-factor authentication for privileged provider and administrator accounts, and SSH keys for server access.
- Role- and tenant-based authorization checks for teachers, classroom sharing, students, results, and parent confirmations.
- Confidentiality commitments and need-based assignment of administrator rights.
- Regular review of access and security measures.

2. Authentication and application security

- Hashed teacher passwords, secure session cookies, and time-limited sessions.
- Random, revocable student and parent access codes. The platform must display and print these codes, so it does not store them as password hashes.
- Hashed sharing-link tokens, limited validity, optional email allowlists, and tiered roles.
- Rate limits for sign-in and API access, plus server-side input validation.

3. Transmission, storage, and separation

- TLS encryption over public networks.
- Logical tenant separation through owner, classroom, exam, and solution identifiers and server-side authorization checks.
- Private exam-image storage. A successful authorization check produces a signed read URL valid for 24 hours.
- Mistral EU endpoint, training opt-out, and Zero Data Retention for optional AI processing.

4. Availability and restoration

- Continuous Litestream replication of the production SQLite database to separate Hetzner object storage.

- Backups retained for no more than 90 days.
- Restoration procedures and regular restoration checks.
- Hosting-provider infrastructure and network protection, with restricted backup access.

5. Logging, incidents, and erasure

- Security and operational logs are limited to required metadata and generally kept for 30 days.
- Exam answers, AI inputs, and AI outputs are not written to application logs.
- Procedures to detect, assess, contain, document, and report security incidents.
- Erasure routines cover database records and related object-storage files. Temporary uploads expire after seven days.
- Regular effectiveness review and adjustment to risk and the state of the art.

Annex 3: Authorized sub-processors

Sub-processor	Location	Service and data	Safeguards
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Germany	Server hosting, production database, object storage, backups, and technical connection data	Article 28 agreement, German data centers, access controls, and documented security measures
Mistral AI SAS, Paris, France	European Union	Optional AI analysis of the exam content listed in Annex 1	Article 28 agreement, EU endpoint, training opt-out, Zero Data Retention, and encrypted transmission

Brevo sends messages for teacher accounts only. Creem processes billing and payments. Those activities belong to purposes for which Intelligrade acts as an independent controller and are not sub-processing of the school data in Annex 1.

Annex 4: Instructions and contacts

Routine instructions are issued through the platform, account settings, and main agreement. Send additional instructions and privacy notices to kevin@intelligrade.de. Intelligrade may verify the identity and authority of the person giving an instruction before acting on it.

Controller's authorized instruction contacts:

Name, role, email:

Signatures

For the Controller

Place, date:

Name, role:

Signature:

For Intelligrade UG (haftungsbeschränkt)

Place, date:

Kevin Peters, Managing Director

Signature:
