

DATA PROCESSING AGREEMENT

Version: 1.3

Effective date: 01.11.2026

Supersedes: version 1.2 of 21.07.2026

Binding Polish original: <https://monteflow.cloud/dpa/1.3/>

Machine translation — for information only. This document is a machine translation of the Polish original. Only the Polish version is binding; in the event of any discrepancy, the Polish text prevails.

This agreement (hereinafter: the **"DPA"**) forms an integral part of the agreement for the provision of the MonteFlow.cloud service concluded between the Parties (hereinafter: the **"Main Agreement"**), i.e.:

- an agreement concluded via the website by accepting the Terms of Service of MonteFlow.cloud for Institutions (hereinafter: the **"Terms of Service"**) and making payment (**"Self-Service Purchase"**), or
- the Agreement for the Provision of the MonteFlow.cloud Service or another agreement concluded individually with the Processor (**"Individual Agreement"**).

The conclusion of the Main Agreement is equivalent to the conclusion of the DPA and does not require a separate signature (§ 14).

§ 1. Parties to the agreement

1. Data controller (principal):

The Controller is the **Institution** — the entity that has concluded the Main Agreement: - in the case of an Individual Agreement — designated as the "Institution" in that agreement, together with the identification, address and contact details specified therein and the person authorised to represent it indicated therein, - in the case of a Self-Service Purchase — designated by the details provided at the time of purchase (name, address of registered office, tax identification number), whose contact address is the e-mail address of the Owner Account within the meaning of the Terms of Service.

Hereinafter referred to as: the **"Controller"** or the **"Institution"**

2. Processor (contractor):

Name: ZUBEL.PRO Krystian Zubel

Legal form: Sole Proprietorship

Registered office address: ul. Orzechowa 5, 55-040 Dobkowice, Polska

NIP (Polish tax identification number): 913-153-70-18

Owner: Krystian Zubel

Contact – general matters: support@monteflow.cloud

Contact – data protection: privacy@monteflow.cloud

Hereinafter referred to as: the **"Processor"** or **"ZUBEL.PRO"**

§ 2. Subject matter and scope of the agreement

1. This Agreement sets out the terms on which the Controller entrusts the processing of personal data to the Processor, in accordance with Art. 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter: the "GDPR").
 2. The Processor processes personal data only on documented instructions from the Controller, to the extent and for the purpose of providing the **MonteFlow.cloud** platform service (hereinafter: the "Service" or the "Platform").
 3. Documented instructions of the Controller include in particular: the provisions of this Agreement, the settings made by the Controller on the Platform (including the choice of operating mode: Basic Mode or Compliance PL Mode), and separate written instructions sent to privacy@monteflow.cloud.
 4. In the event of any discrepancy between the documents, the order of precedence set out in the Individual Agreement applies, and in its absence — the order set out in § 19(2) of the Terms of Service.
 5. If the Controller has its registered office outside the European Economic Area, the data are processed by the Processor in the European Union in accordance with this Agreement and the GDPR. The Controller is responsible for the compliance of the processing with the law applicable at its registered office, including for transfers of data that it itself exports from the Platform. To the extent required by Chapter V of the GDPR, the transfer of data by the Processor to the Controller is governed by the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914 (Module Four: transfer processor to controller), which the Parties deem to be incorporated into this Agreement.
-

§ 3. Details of processing

1. Subject matter and nature of processing

The Processor processes personal data in connection with the provision of the Service, which comprises: storing data entered by the Controller and users of the Platform, making data available to authorised users, making backups, ensuring the continuity and security of the Service and, in Compliance PL Mode, generating documentation required by the provisions of education law.

2. Duration of processing

Processing continues for the term of the Main Agreement, taking into account the transitional periods set out in § 9.

3. Categories of data subjects

The Processor processes data of the following categories of persons:

- participants of activities conducted by the Institution (pupils, students, training participants), including children,
- parents and legal guardians of children,
- teachers, staff and associates of the Institution.

4. Categories of personal data processed

Data concerning participants (pupils, students, training participants, including children):

- first name and surname,
- date of birth,
- image (photographs — if entered by the Institution),
- pedagogical observations,
- attendance information,
- data concerning skills and progress,
- allergens and other data concerning health (if entered by the Institution),
- other data voluntarily entered by the Institution.

Data concerning parents/legal guardians:

- first name and surname,
- e-mail address,
- telephone number,
- identity document number,
- authentication data (account identifier),
- other data voluntarily entered by the Institution.

Data concerning teachers and staff of the Institution:

- first name and surname,
- e-mail address,
- authentication data (account identifier),
- information on the role/position in the Institution.

Data from audit logs (audit trail): - identifier of the user performing the operation, - type of operation (read, write, modification, deletion), - date and time of the operation, - identifier of the object to which the operation related (e.g. child identifier, observation identifier).

5. Special categories of data (Art. 9 GDPR)

1. The Platform enables the Controller to enter data concerning children's health (in particular information on allergens and health conditions). These data constitute special categories of personal data within the meaning of Art. 9(1) GDPR.
 2. The Controller is solely responsible for having an appropriate legal basis for processing special categories of data (in particular the explicit consent of a parent/legal guardian or the performance of the Institution's legal obligations).
 3. The Processor applies to special categories of data the same protection measures as to other data, in particular encryption, role-based access control and isolation of data between institutions.
 4. The Processor applies to special categories of data restrictive access control that allows access to such data only for users with School Administrator access and Teachers assigned to the groups or courses that the child attends. The School Administrator may expressly grant access to such data to other accounts via the Platform.
-

§ 4. Purpose of processing

1. The Processor processes personal data solely for the following purposes:
 - provision of the MonteFlow.cloud platform Service,
 - maintaining the security and continuity of operation of the system,
 - making and storing backups,
 - resolving technical problems reported by the Controller or users,
 - keeping audit logs documenting operations on personal data, in order to ensure accountability and security of processing (Art. 5(2) and Art. 32 GDPR),
 - in Compliance PL Mode — generating documentation required by the provisions of education law, on the instruction of the Controller.
 2. The Processor does not process personal data for its own purposes; in particular, it does not use the data for profiling, analytics, marketing, artificial intelligence or disclosure to third parties.
 3. The Controller is solely responsible for having an appropriate legal basis for the processing of personal data (Art. 6 and Art. 9 GDPR) and for the compliance of the processing with the provisions of education law.
 4. In Compliance PL Mode, the provisions of education law may specify additional purposes and retention periods for educational documentation. The Controller is responsible for determining those purposes and periods, and the Processor implements them on its documented instructions.
-

§ 5. Obligations of the Processor

1. General obligations

1. The Processor undertakes to:

- process personal data only on documented instructions from the Controller, unless required to do so by EU law or Polish law — in such a case, the Processor informs the Controller of that legal requirement before processing (unless that law prohibits this),
- ensure that persons authorised to process personal data have committed themselves to confidentiality,
- implement the appropriate technical and organisational measures set out in Annex A,
- comply with the conditions for engaging sub-processors set out in § 7,
- assist the Controller in fulfilling its obligations towards data subjects (Articles 15–22 GDPR),
- assist the Controller in fulfilling the obligations set out in Articles 32–36 GDPR (security, breach notification, impact assessment),
- after the end of the provision of the Service, delete or return the data in accordance with § 9,
- make available to the Controller the information necessary to demonstrate compliance with Art. 28 GDPR.

2. The Processor promptly informs the Controller if, in its opinion, an instruction of the Controller infringes the GDPR or other data protection provisions (Art. 28(3) second subparagraph GDPR).

2. Data security

1. The Processor has implemented and maintains the technical and organisational measures described in detail in Annex A, ensuring a level of security appropriate to the risk associated with the processing.
2. The Processor undertakes to regularly review and update the security measures applied in order to ensure their adequacy in the face of changing threats.
3. The Processor informs the Controller of material changes to the security measures applied at least 14 days in advance.

3. Assistance with data subjects' rights

1. The Processor, taking into account the nature of the processing, assists the Controller in fulfilling the obligations arising from Articles 15–22 GDPR, in particular by making available Platform tools enabling the export, modification and deletion of data.
 2. The Processor promptly forwards to the Controller all requests from data subjects addressed directly to the Processor, without responding to such requests itself.
 3. The Controller is responsible for handling data subjects' requests and for responding to them within the time limits required by the GDPR.
-

§ 6. Obligations of the Controller

1. The Controller undertakes to:
 - have an appropriate legal basis for processing the personal data entrusted to the Processor,
 - inform data subjects of the processing of their data on the Platform,
 - issue to the Processor only instructions compliant with data protection provisions,
 - promptly notify the Processor of any changes in the scope or purpose of processing,
 - take care of the security of the access credentials to the Platform (in particular the login credentials of the Institution's users),
 - handle requests and complaints from data subjects.
 2. The Controller is solely responsible for the compliance of the data processing with the law (the GDPR, education regulations, other applicable regulations), including for obtaining the required consents.
-

§ 7. Sub-processors (further entrustment of processing)

1. General authorisation and list of sub-processors

1. The Controller gives general authorisation for the Processor to use the sub-processors listed in Annex B to this Agreement.
2. Identity providers used for optional social login (Apple, Google) are not sub-processors within the meaning of this Agreement. By choosing this login method, the User authenticates using their own account with the provider, which processes the data as an independent controller, on the basis of its own terms. The Processor does not entrust data covered by this Agreement to those entities.
3. As at the date of conclusion of the Agreement, the Processor uses the following sub-processors:

Sub-processor	Registered office	Data location	Function	Transfer basis
Amazon Web Services EMEA SARL	Luxembourg (EU)	Servers in the EU (eu-north-1 - Stockholm, Sweden; eu-south-1 - Milan, Italy)	Hosting, data storage, cloud infrastructure	Processing in the EEA; AWS Inc. (USA) as a sub-sub-processor covered by the EU-US Data Privacy Framework

Sub-processor	Registered office	Data location	Function	Transfer basis
Apple Distribution International Ltd	Cork, Ireland (EU)	APNs infrastructure (EU/USA)	Delivery of push notifications to the iOS mobile application — when the iOS mobile application with push notifications is available	Processing in the EEA; Apple Inc. (USA) as a sub-sub-processor covered by the EU-US Data Privacy Framework
Google Cloud EMEA Limited	Dublin, Ireland (EU)	FCM infrastructure (EU/USA)	Delivery of push notifications to the Android mobile application — when the Android mobile application with push notifications is available	Processing in the EEA; Google LLC (USA) as a sub-sub-processor covered by the EU-US Data Privacy Framework

The mobile application is in the testing phase and is planned to be made available to users in 2026. The content of push notifications is minimised — it does not contain data concerning health or other special categories of data.

2. Procedure for changing sub-processors

1. The Processor informs the Controller of its intention to engage a new sub-processor or replace an existing one at least **30 days** in advance, by e-mail to the Controller's contact address (§ 1(1)).
2. The Controller may raise a justified objection to the new sub-processor within **14 days** of receiving the notification.
3. In the event of an objection, the Processor will make reasonable efforts to propose an alternative solution. If the parties do not reach agreement within 30 days of the objection being raised, the Controller has the right to terminate the Main Agreement with immediate effect.
4. The Processor ensures that each sub-processor is bound by data protection obligations no less stringent than those set out in this Agreement.

§ 8. Personal data breaches

1. In the event that a personal data breach is detected (Articles 33–34 GDPR), the Processor notifies the Controller promptly, no later than within **36 hours** of detecting the breach, providing at least the following information:
 - a description of the nature of the breach,
 - the categories and approximate number of data subjects concerned,
 - the likely consequences of the breach,
 - a description of the remedial measures taken or proposed.

2. If full information is not available at the time of the first notification, the Processor provides it in phases, without undue delay.
 3. The Processor supports the Controller in fulfilling the obligations to notify the breach to the supervisory authority (UODO) and to communicate it to the data subjects.
 4. The Processor documents all personal data breaches, including the circumstances of the breach, its effects and the remedial action taken.
-

§ 9. Deletion and return of data after termination of the agreement

1. After the Main Agreement ends and the licence expires, the Processor provides the Controller with a 30-day period of access in read-only mode, enabling data export. The validity of the licence after the Main Agreement ends is specified in the Terms of Service (§ 12(1)) or in the Individual Agreement.
2. After the read-only period has elapsed, on the instruction of the Controller, the Processor without undue delay:
 - returns all personal data in a structured format (CSV, JSON or XML), or
 - deletes all personal data from the production servers.
3. In the absence of an express instruction from the Controller within 30 days of the end of the read-only period, the Processor deletes all personal data from the production servers. On the Controller's written instruction, deletion may take place earlier, including before the end of the read-only period.
4. Data in backups are automatically deleted within **90 days** of deletion from the production system, in accordance with the backup rotation cycle.
5. **Data retained after deletion.** When deleting data in accordance with sec. 2 or 3, the Processor retains only:
 1. **an archive of the full data export — only for Controllers using Compliance PL Mode.** The archive is prepared and verified before any data are deleted, stored for **90 days** from deletion solely for the purpose of returning it to the Controller on request (sec. 2), and then automatically deleted. For Controllers not using Compliance PL Mode, no archive is prepared;
 2. **billing data** — licences, invoices and corrective invoices, events received from the payment operator, results of VAT number verifications and the Controller's identification data for billing purposes (name, tax identification number, address, billing e-mail address, payment and invoice identifiers). The Processor processes these data as a controller, in accordance with the Privacy Policy, for 18 months; documentation required by tax regulations is stored by the invoicing and payment systems referred to in the Privacy Policy;
 3. **the system event log (audit)** — until the retention period of the individual entries expires; entries documenting the granting of permissions, the deletion of data at the request of a data subject, the recording of Health Consent and the deletion of the Controller's data itself are stored for 10 years as evidence of accountability (Art. 5(2) GDPR);

4. **backups** — until they expire in accordance with sec. 4.
6. Accounts of users belonging exclusively to the Controller whose data are being deleted are deleted. A user who also belongs to another institution using the Platform retains their account and loses access to the Controller's data; that user's data relating to the other institution are processed on the instruction of that institution as a separate controller.
7. After the data are deleted, the Processor sends the Controller, to the contact address and the billing e-mail address, a confirmation of deletion together with information on the data retained in accordance with sec. 5.
8. In Compliance PL Mode, the Controller is responsible for exporting the data required by the provisions of education law before the end of the read-only period. The archive referred to in sec. 5 item 1 does not replace this obligation. The Processor is not liable for the Controller's failure to export data.
9. The Processor may retain data if EU law or Polish law requires further storage — in such a case, the Processor informs the Controller of the legal basis for such storage.
-

§ 10. Audits and inspections

1. The Processor makes available to the Controller the information necessary to demonstrate compliance with the obligations arising from Art. 28 GDPR and enables audits and inspections to be carried out.
2. Audits and inspections take place on the following terms:
- the Controller notifies its intention to carry out an audit at least **14 days** in advance,
 - audits are carried out during the Processor's working hours (Monday–Friday, 9:00–17:00),
 - scheduled audits are carried out no more often than **once per calendar year**, unless the audit is related to a specific personal data breach,
 - the auditor is obliged to maintain confidentiality with respect to the data of the Processor's other customers,
 - the costs of the audit are borne by the Controller, unless the audit reveals a material breach of the Processor's obligations.
3. At the Controller's request, the Processor makes available documentation concerning the security measures applied as described in Annex A.
-

§ 11. Liability

1. The liability of the parties for breach of the obligations arising from this Agreement is governed by the provisions of the GDPR (in particular Art. 82) and the Polish Civil Code (Kodeks cywilny).
2. The Processor is not liable for breaches caused by:
- acts or omissions of the Controller, its employees or users of the Platform,

- instructions of the Controller that do not comply with the GDPR, of which the Processor has informed the Controller in accordance with § 5(2),
 - the Controller's failure to export data within the time limits set out in § 9.
3. The Processor's total liability for damages towards the Controller under this Agreement is limited to an amount equal to the sum of the fees paid by the Controller to the Processor in the **12 months** preceding the event giving rise to the claim. This limitation does not apply to damage caused intentionally and does not infringe mandatory provisions of law.
-

§ 12. Term and amendments of the agreement

1. The DPA enters into force on the date of conclusion of the Main Agreement and remains in force for its duration.
 2. The Processor publishes each subsequent version of the DPA at a separate, permanent address and maintains an archive of earlier versions. Published versions are not subject to change. The Parties are bound by the version indicated in accordance with § 14(2), until it is amended under the procedure in sec. 3–5.
 3. If the Processor intends to introduce changes materially affecting the terms of data processing, it informs the Controller by e-mail to the contact address (§ 1(1)) at least **30 days** in advance, indicating the scope of and justification for the changes. The Controller may raise an objection within **14 days** of receiving the notification. The absence of an objection within that period constitutes acceptance of the changes.
 4. If an objection is raised, the Parties will enter into negotiations; until they are concluded, the Parties are bound by the existing version of the DPA. If the Parties do not reach agreement within 30 days of the objection being raised, the Controller has the right to terminate the Main Agreement with immediate effect, without incurring any liability on that account.
 5. Changes other than those specified in sec. 3 — in particular editorial corrections, updates of contact details and changes resulting from changes in generally applicable law — may be introduced by the Processor upon publication, informing the Controller of them in the next notification.
 6. Changes to the list of sub-processors are subject exclusively to the procedure set out in § 7(2).
 7. The Processor's obligations concerning confidentiality and data security also apply after the DPA ends.
-

§ 13. Final provisions

1. **Confidentiality:** The Processor undertakes to keep confidential all information received from the Controller, including the content of the personal data processed. The confidentiality obligation is not limited in time.
2. **Governing law:** The Agreement is governed by Polish law.

3. **Dispute resolution:** The parties will endeavour to resolve all disputes arising from the Agreement amicably. If no agreement is reached, disputes will be resolved by the common court having jurisdiction over the Processor's registered office.
 4. **Severability clause:** If any provision of the Agreement is found to be invalid or ineffective, the remaining provisions remain in force. The Parties will replace the invalid provision with a provision closest to the economic purpose of the invalid provision.
 5. This Agreement together with its annexes constitutes the entire agreement of the parties with respect to the entrustment of the processing of personal data and supersedes all prior arrangements in this respect.
-

§ 14. Conclusion of the DPA

1. This DPA is concluded together with the Main Agreement and does not require separate signatures of the Parties; electronic form is sufficient (Art. 28(9) GDPR):
 - in the case of a Self-Service Purchase — at the moment the agreement is concluded in accordance with the Terms of Service, after acceptance of the Terms of Service, which provide for the conclusion of the DPA,
 - in the case of an Individual Agreement — at the moment of its conclusion.
 2. The Parties are bound by the version of the DPA:
 - in the case of a Self-Service Purchase — the version published as the current version at the time the Terms of Service are accepted, even if, for Controllers who concluded the Main Agreement earlier, it takes effect at a later date in accordance with § 12(3); the Processor records the date of acceptance and the version of the DPA and sends the Controller a confirmation containing a link to that version,
 - in the case of an Individual Agreement — indicated in that agreement,and in each case — a version introduced later under the procedure in § 12(3)–(5).
-

ANNEX A: TECHNICAL AND ORGANISATIONAL MEASURES

A.1. Technical measures

- Encryption of data in transit (TLS 1.2+).
- Encryption of data at rest (AES-256, managed by AWS).
- Geo-redundant data storage (at least 2 availability zones in the EU region).
- Daily automatic backups with retention of up to 90 days.
- Role-based access control (RBAC) with the principle of least privilege.
- Logging and monitoring of data access and system changes (audit trail).
- Multi-factor authentication (MFA) for administrative accounts.

- Isolation of the data of different institutions at database level (tenant isolation).
- Infrastructure protection provided by AWS (firewall, DDoS protection, physical security of data centres).
- Regular updates of software and dependencies.

A.2. Organisational measures

- Principle of least privilege — only persons for whom it is necessary for the provision of the Service have access to personal data.
- Confidentiality undertakings from all persons with access to the data.
- Access management procedures (granting and revoking permissions).
- Security incident management procedures.
- Procedures for making, verifying and restoring backups.
- Procedures for handling data subject requests.
- Regular reviews of the security measures applied.

A.3. Location of processing

All personal data are stored and processed on AWS servers located in the European Union:

- **Primary region:** eu-north-1 (Stockholm, Sweden)
- **Backup region:** eu-south-1 (Milan, Italy)

ANNEX B: LIST OF SUB-PROCESSORS

Sub-processor	Registered office	Data location	Function	Transfer basis (if outside the EEA)
Amazon Web Services EMEA SARL	Luxembourg (EU)	eu-north-1, eu-south-1 (EU)	Hosting, computing, data storage, cloud infrastructure (Lambda, DynamoDB, S3, CloudFront, Cognito, API Gateway, SNS)	Processing in the EEA. AWS Inc. (USA) as a sub-sub-processor: EU-US Data Privacy Framework
Apple Distribution International Ltd	Cork, Ireland (EU)	APNs infrastructure (EU/USA)	Delivery of push notifications to the iOS mobile application — when the iOS mobile application with push notifications is available	Processing in the EEA. Apple Inc. (USA) as a sub-sub-processor: EU-US Data Privacy Framework

Sub-processor	Registered office	Data location	Function	Transfer basis (if outside the EEA)
Google Cloud EMEA Limited	Dublin, Ireland (EU)	FCM infrastructure (EU/USA)	Delivery of push notifications to the Android mobile application — when the Android mobile application with push notifications is available	Processing in the EEA. Google LLC (USA) as a sub-sub-processor: EU-US Data Privacy Framework

The mobile application is in the testing phase and is planned to be made available to users in 2026. The content of push notifications is minimised — it does not contain data concerning health or other special categories of data.

Identity providers used for optional social login (Apple, Google) are not sub-processors — they process data as independent controllers, in accordance with § 7(1) item 2.

The Controller consents to the sub-processors listed above as of the date of conclusion of this Agreement. Changes to the list of sub-processors are subject to the procedure set out in § 7.2.

Version: 1.3 · **Effective date:** 01.11.2026 · **Supersedes:** version 1.2 of 21.07.2026

ZUBEL.PRO Krystian Zubel

ul. Orzechowa 5, 55-040 Dobkowice

NIP: 913-153-70-18

support@monteflow.cloud | privacy@monteflow.cloud