

PRIVACY POLICY OF THE MONTEFLOW.CLOUD PLATFORM

Last updated: 1 November 2026

Version: 1.3

Supersedes: version 1.2 of 21 July 2026

Binding Polish original: <https://monteflow.cloud/privacy/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.

§ 1. General information

1. This Privacy Policy sets out the rules for the processing of personal data in connection with the use of the MonteFlow.cloud platform (hereinafter: the "Platform") operated by:

ZUBEL.PRO Krystian Zubel

Sole proprietorship

ul. Orzechowa 5, 55-040 Dobkowice, Poland

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

General contact: support@monteflow.cloud Data protection contact: privacy@monteflow.cloud

Hereinafter: "ZUBEL.PRO", "we" or the "Operator".

2. In connection with the Platform, ZUBEL.PRO acts in two separate roles within the meaning of the GDPR:
 - **Controller** — with respect to personal data collected in its own name and for its own purposes (data of representatives of Institutions, billing data, technical data related to the operation of the Platform). Details in § 3.
 - **Processor** — with respect to personal data entered into the Platform by Institutions (data of children, parents, teachers). Details in § 4.
3. This Policy applies to all persons who use the Platform or whose data are processed in it: representatives of Institutions, persons purchasing the Service through the website, teachers and staff, parents and legal guardians, and participants in activities (pupils, students, training participants, including children).

§ 2. Definitions

For the purposes of this Privacy Policy, the following terms have the following meanings:

- **GDPR** — 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.
 - **Platform** — the MonteFlow.cloud website together with related services.
 - **Institution** — a kindergarten, school or other educational institution using the Platform on the basis of an agreement with ZUBEL.PRO.
 - **User** — any person holding an account on the Platform (teacher, parent, legal guardian, employee of an Institution).
 - **Entrusted data** — personal data entered into the Platform by an Institution or its Users, for which the Institution is the controller.
-

§ 3. ZUBEL.PRO as controller

1. What data we collect as controller

As part of its own business, ZUBEL.PRO collects and processes the following categories of personal data:

1. Data of representatives of Institutions (B2B customers):

- first name and surname of the person representing the Institution,
- position/function in the Institution,
- business e-mail address,
- business telephone number,
- Institution data: name, registered office address, NIP, REGON.

2. Billing data and data relating to purchases through the website:

- data necessary to issue an invoice (name of the Institution, registered office address, country, NIP or EU VAT number),
- first name, surname and e-mail address of the person making the purchase (this address becomes the address of the Owner Account and the billing e-mail address), telephone number, if provided,
- customer, subscription and payment identifiers assigned by the payment operator (Stripe) and the invoicing system (inFakt), the invoice number and the KSeF number,
- limited payment method data provided by the payment operator (card type and brand, last four digits, expiry date) — ZUBEL.PRO does not receive the full card number or the CVC code,
- payment events (e.g. payment made, failed charge, refund, disputed payment), the selected package, the Licence Limit and the billing period,
- the result of the verification of the EU VAT number in the VIES system,

- the record of acceptance of the Terms of Service and the Privacy Policy at the time of purchase (date, time, document versions),
- payment and invoice history.

3. Data related to the User account:

- e-mail address used for registration,
- account identifier,
- date of registration and of last login,
- account preferences (language, notifications).

4. Technical and analytical data:

- IP address,
- browser type and version,
- operating system,
- dates and times of access to the Platform,
- system logs relating to security and diagnostics.

5. Newsletter subscriber data:

- e-mail address,
- first name (if provided),
- name of the Institution (if provided),
- date of addition to the subscriber list,
- source of acquisition (form on the MonteFlow.cloud website or direct provision of the address by the subscriber).

2. Purposes and legal bases of processing

Purpose of processing	Categories of data	Legal basis	Retention period
Conclusion and performance of the agreement for the provision of the Service	Data of representatives of Institutions, billing data	Art. 6(1)(b) GDPR (performance of a contract)	Term of the agreement + 30 days
Conclusion of the agreement through the website, handling of recurring payments, changes to the Licence Limit and cancellations	Billing data and purchase data	Art. 6(1)(b) GDPR (conclusion and performance of a contract)	Term of the agreement; thereafter in accordance with the row "Issuing invoices"

Purpose of processing	Categories of data	Legal basis	Retention period
Issuing invoices, submitting them to the National e-Invoicing System (KSeF) and tax settlements, verification of EU VAT numbers in the VIES system, recording of sales for the purposes of VAT thresholds	Billing data	Art. 6(1)(c) GDPR (legal obligation — Polish VAT Act, Polish Tax Ordinance, Polish Accounting Act)	Copies in ZUBEL.PRO's systems: up to 18 months from their creation (identification data of the Institution — up to 18 months from the deletion of its data from the Platform). Invoices and tax documentation: 5 years from the end of the calendar year in which the tax payment deadline expired — stored in the invoicing system (inFakt), in KSeF and with the payment operator (Stripe)
Demonstrating the conclusion of the agreement and the acceptance of the Terms of Service	Acceptance record, purchase data	Art. 6(1)(f) GDPR (legitimate interest — establishment, exercise and defence of legal claims)	Term of the agreement + limitation period for claims
Prevention of payment fraud and abuse at purchase	Purchase data, payment method data, IP address	Art. 6(1)(f) GDPR (legitimate interest — transaction security)	In accordance with the periods specified for billing data and technical data
Operational contact with the Institution (technical support, notifications of changes)	Contact data of representatives	Art. 6(1)(f) GDPR (legitimate interest — performance of the agreement and ongoing communication)	Term of the agreement + 30 days
Maintaining and operating the User account	User account data	Art. 6(1)(b) GDPR (performance of a contract / provision of the service)	Duration of the account + 30 days
Ensuring the security of the Platform, diagnostics, detection of abuse	Technical data, logs	Art. 6(1)(f) GDPR (legitimate interest — system security)	Up to 18 months from recording
Establishment or defence of claims	Contact data, billing data, logs	Art. 6(1)(f) GDPR (legitimate interest)	Limitation period for claims (as a rule, 3 years)

Purpose of processing	Categories of data	Legal basis	Retention period
Sending product newsletters (information about new features of the Platform) to representatives of Institutions and interested persons	E-mail address, first name, name of the Institution (if provided), source of acquisition	Art. 6(1)(f) GDPR (legitimate interest — direct marketing to customers and to persons who voluntarily provided their e-mail address with a view to receiving such messages) in conjunction with Art. 10 of the Polish Act on the Provision of Electronic Services	Until an objection is raised or the person unsubscribes from the list; no longer than 3 years from the last interaction

3. Legitimate interests

Where processing is based on Art. 6(1)(f) GDPR, the legitimate interests of ZUBEL.PRO comprise: ongoing communication with customers necessary for the performance of the agreement, ensuring the security and continuity of the Platform's operation, prevention of payment fraud, demonstrating the conclusion of the agreement, and the establishment or defence of claims. Data subjects have the right to object to such processing (see § 6).

§ 4. ZUBEL.PRO as processor

1. Data entrusted by Institutions

Institutions using the Platform enter into it personal data of children (pupils/students), parents and legal guardians, as well as teachers and staff. **The controller of these data is the Institution, not ZUBEL.PRO.**

ZUBEL.PRO processes these data solely on documented instructions from the Institution, on the basis of the Data Processing Agreement (DPA) concluded with each Institution.

2. Scope of entrusted data

The detailed scope of entrusted data is specified in the DPA concluded with the Institution. These data may include in particular:

- identification data of children (first name, surname, date of birth),
- image of children (photographs),
- pedagogical observations and progress data,
- attendance information,
- health data — allergens, health conditions, health notes (up to 2,000 characters), designation of special educational needs (SEN) and sensitive SEN documents (files) — constituting special categories of data within the meaning of Art. 9 GDPR; entering them into the Platform requires prior registration of the Health Consent of the parent/guardian,

- contact data of parents/guardians (first name, surname, e-mail, telephone),
- data of teachers (first name, surname, e-mail, role in the Institution).

3. Rules for processing entrusted data

1. ZUBEL.PRO processes entrusted data solely for the purpose of providing the Service to the Institution and in accordance with its instructions.
2. ZUBEL.PRO does not use entrusted data for its own purposes; in particular, it does not use them for profiling, analytics, marketing or artificial intelligence.
3. Any requests concerning entrusted data (access, rectification, erasure, portability) should be addressed directly to the Institution, which is their controller. ZUBEL.PRO supports the Institution in handling such requests to the extent specified in the DPA.

4. Entrusted data after termination of the agreement with the Institution

After termination of the agreement with the Institution and expiry of the read-only access period, entrusted data are deleted in accordance with § 9 of the DPA. After deletion, ZUBEL.PRO retains only:

- for Institutions using the Compliance PL Mode — an archive of the full data export for 90 days, solely for the purpose of returning it to the Institution, after which the archive is automatically deleted; for other Institutions no archive is created,
- the system event log (audit) — until the expiry of the retention period of the entries; entries documenting the granting of permissions, the deletion of data and the registration of the Health Consent — for 10 years,
- backup copies — until their expiry, no longer than 90 days from the deletion of the data,
- billing data of the Institution, processed by ZUBEL.PRO as controller in accordance with § 3.

Accounts of persons belonging exclusively to that Institution are deleted. Persons who also belong to another Institution using the Platform retain their account and lose access to the data of the Institution whose agreement has ended.

5. Contact regarding entrusted data

If you are a parent, legal guardian, teacher or other person whose data have been entered into the Platform by an Institution, and you wish to exercise your rights under the GDPR, please contact the Institution, which is the controller of your data. The Institution is obliged to respond to your request. If you have difficulty obtaining a response from the Institution, you may also contact us at privacy@monteflow.cloud — we will forward your request to the Institution.

§ 5. Recipients of data

1. Recipients of data for which ZUBEL.PRO is the controller

ZUBEL.PRO may disclose personal data for which it is the controller to the following categories of recipients:

- **Amazon Web Services EMEA SARL** (Luxembourg — EU) — cloud infrastructure provider; for users from the EU, the contracting party and processor is this entity established in the EU. Data are stored on servers in the EU (Stockholm, Milan). Any access by Amazon Web Services, Inc. (USA) as a group entity is covered by the EU-US Data Privacy Framework.
- **Slack Technologies (Salesforce)** — communication platform used for ongoing communication with representatives of Institutions (§ 3(6) of the Agreement). Data processed: first name, surname (or pseudonym) and e-mail address of the person designated by the Institution. Data processed on the basis of Art. 6(1)(f) GDPR (legitimate interest — ongoing communication with the customer). Slack Inc., established in the USA, is covered by the EU-US Data Privacy Framework.
- **Apple Distribution International Ltd** (Cork, Ireland — EU) — e-mail hosting provider for the company mailboxes support@monteflow.cloud and privacy@monteflow.cloud (iCloud with a custom domain). For users from the EU, the contracting party and the entity responsible for processing is this entity established in the EU. Data processed: content of correspondence and contact data of persons writing to us. Any access by Apple Inc. (USA) as an entity of the Apple group takes place on the basis of standard contractual clauses (SCC).
- **MailerLite (MailerLite, UAB)** — tool for sending product newsletters and managing the subscriber list. Data processed: e-mail address, first name, name of the Institution (if provided), subscription status. Registered office: Paupio g. 46, Vilnius, Lithuania (EU). Processing within the European Economic Area; any sub-sub-processors in the USA are covered by the EU-US Data Privacy Framework.
- **Stripe Payments Europe, Limited** (Dublin, Ireland — EU) — payment operator for purchases made through the website: handling of the payment form, recurring payments, tax calculation and VAT number verification, and the Customer Portal. Data processed: billing data and purchase data, payment method data (full card data go exclusively to Stripe). With respect to subscription handling, Stripe acts on behalf of ZUBEL.PRO, and with respect to the execution of payment transactions, fraud prevention and obligations under the legislation on payment services and anti-money laundering — as an independent controller, on the basis of its own privacy policy: <https://stripe.com/privacy>. Any access by Stripe, Inc. (USA) is covered by the EU-US Data Privacy Framework and by standard contractual clauses (SCC).
- **inFakt Sp. z o.o.** (Kraków, Poland) — invoicing system: issuing invoices and corrective invoices and submitting them to KSeF on behalf of ZUBEL.PRO. Data processed: data necessary to issue an invoice. Processing in Poland, on the basis of a data processing agreement.
- **Biuro Rachunkowe Małe Podatki** (malepodatki.pl, Poland) — with respect to billing data necessary for bookkeeping and tax settlements, on the basis of a separate data processing agreement.
- **National e-Invoicing System (KSeF), operated by the minister competent for public finance** — recipient of all invoices and corrective invoices issued by ZUBEL.PRO, including invoices for foreign purchasers, on the basis of Art. 6(1)(c) GDPR in conjunction with the provisions of the Polish VAT Act.

- **VIES system (European Commission and the tax administrations of EU Member States)** — with respect to the verification of the EU VAT number provided at purchase; the purchaser's VAT number and ZUBEL.PRO's VAT number are transmitted.
- **Public authorities** — to the extent required by applicable law (e.g. tax authorities).

ZUBEL.PRO does not sell personal data and does not disclose them to third parties for marketing purposes.

2. Recipients of entrusted data

Data entrusted by Institutions are not disclosed by ZUBEL.PRO to any third parties, except for the sub-processors listed in the DPA (in particular AWS as infrastructure provider). Once the mobile application with push notifications is made available, the sub-processors will also include Apple Distribution International Ltd (Cork, Ireland — EU) with respect to notifications to iOS devices and Google Cloud EMEA Limited (Dublin, Ireland — EU) with respect to notifications to Android devices; the content of notifications is minimised and does not contain health data or other special categories of data. The list of current sub-processors is available in the DPA concluded with the Institution.

3. Social login (Apple, Google)

The Platform allows optional login using an Apple or Google account. Choosing this login method is voluntary — the alternative is login with an e-mail address and password.

When using social login, you authenticate directly with the selected provider using your own account. Only the confirmation of identity together with the e-mail address and first name (if you share them with the provider) is transmitted to the Platform. ZUBEL.PRO does not receive your password.

Apple and Google process data related to such login as **independent controllers**, on the basis of their own terms and privacy policies — they are not sub-processors of ZUBEL.PRO and we do not entrust them with data processed in the Platform. The rules for the processing of data by these providers are set out in:

- Apple: <https://www.apple.com/legal/privacy/>
- Google: <https://policies.google.com/privacy>

§ 6. Rights of data subjects

1. Rights with respect to data controlled by ZUBEL.PRO

If ZUBEL.PRO is the controller of your data (data of representatives of Institutions, User account data, technical data), you have the following rights:

- **Right of access** (Art. 15 GDPR) — the right to obtain information about the processing of your data and a copy of the data.
- **Right to rectification** (Art. 16 GDPR) — the right to have inaccurate data corrected or incomplete data completed.

- **Right to erasure** (Art. 17 GDPR) — the right to request erasure of data, subject to the exceptions provided for in the GDPR (e.g. tax obligations).
- **Right to restriction of processing** (Art. 18 GDPR) — the right to request restriction of processing in certain cases.
- **Right to data portability** (Art. 20 GDPR) — the right to receive data in a structured, commonly used format.
- **Right to object** (Art. 21 GDPR) — the right to object to processing based on legitimate interest (Art. 6(1)(f) GDPR).
- **Right to lodge a complaint** — the right to lodge a complaint with the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych, UODO) (ul. Stawki 2, 00-193 Warszawa, www.uodo.gov.pl).

In particular, with respect to product newsletters sent via MailerLite — the processing is based on Art. 6(1)(f) GDPR (legitimate interest), and you therefore have the right to object (Art. 21 GDPR) at any time. You may unsubscribe from the subscriber list at any time by clicking the unsubscribe link in each newsletter message or by contacting privacy@monteflow.cloud.

2. Rights with respect to entrusted data (data in the Platform)

If your data have been entered into the Platform by an Institution (data of children, parents, teachers), the controller of these data is the Institution. Any requests concerning these data should be addressed to the Institution. ZUBEL.PRO is not authorised to handle such requests on its own.

3. How to exercise your rights

Requests concerning data for which ZUBEL.PRO is the controller should be sent to: privacy@monteflow.cloud. A response will be given without undue delay, and no later than within 30 days of receipt of the request. In justified cases, this period may be extended by a further 60 days, of which the person will be informed.

§ 7. International data transfers

1. Data entrusted by Institutions are stored on AWS servers located in the European Union (regions: eu-north-1 — Stockholm, Sweden; eu-south-1 — Milan, Italy).
2. With the exception of Slack Technologies (USA), the service providers listed in § 5 (excluding KSeF, the VIES system and public authorities) are established in the European Union and are the contracting party for users from the EU. The transfer of data to Slack Technologies and limited access by entities of the same corporate groups established in the USA (in particular Amazon Web Services, Inc., Apple Inc. and Stripe, Inc.) — as sub-sub-processors or for the purposes of infrastructure maintenance and payment handling — are covered by the **EU-US Data Privacy Framework** (implementing decision of the European Commission of 10 July 2023), and in the case of Apple Inc. and Stripe, Inc. additionally by standard contractual clauses (SCC).

3. Apart from the cases indicated in § 5 and in sec. 2 above, ZUBEL.PRO does not transfer personal data to third countries. Should such a transfer become necessary in the future, ZUBEL.PRO will ensure an adequate level of protection in accordance with Chapter V GDPR and will provide information about it in an updated Privacy Policy.
4. Social login (§ 5(3)) does not constitute a transfer of entrusted data — Apple and Google process authentication data as independent controllers, on the basis of their own privacy policies.
-

§ 8. Cookies and tracking technologies

1. Types of cookies used

Type	Purpose	Legal basis	Retention period
Strictly necessary cookies (session)	Maintaining the login session, security, basic operation of the Platform	Art. 6(1)(f) GDPR (technical necessity)	Until the end of the session
Strictly necessary cookies of the payment operator (Stripe) — only on the pricing page and in the payment form	Displaying the purchase form, prevention of payment fraud, transaction security	Art. 6(1)(f) GDPR (necessity for the provision of the service requested by the user)	In accordance with Stripe's policy: https://stripe.com/cookies-policy/legal

2. What we do not use

The Platform **does not use**:

- marketing or advertising cookies,
- tools for tracking user behaviour (tracking),
- tracking pixels,
- third-party analytics tools (e.g. Google Analytics); the Stripe cookies listed in the table above serve solely for payment handling and fraud prevention,
- user profiling.

3. Managing cookies

The User may manage cookies via the settings of their browser. Disabling strictly necessary cookies may make it impossible to use the Platform.

§ 9. Data security

ZUBEL.PRO applies appropriate technical and organisational measures to protect personal data, in particular:

- encryption of data in transit (TLS 1.2+) and at rest (AES-256),
 - role-based access control following the principle of least privilege,
 - multi-factor authentication (MFA) for privileged accounts, in accordance with the Platform's MFA policy,
 - isolation of the data of different Institutions at database level,
 - logging and monitoring of access,
 - daily automatic backups, replicated to a second EU region (geo-redundancy),
 - regular security reviews and updates.
-

§ 10. Children's data

1. ZUBEL.PRO does not itself collect personal data of children. Children's data are entered into the Platform by Institutions, which are their controllers.
 2. The Platform is not directed at children, and children do not register on it themselves. An account for a participant in activities, including a child, may be created only by the Institution (within the Roles and Permissions Module), which is responsible for the legal basis for its creation.
 3. All matters relating to the processing of children's data, including obtaining the required consents, are the responsibility of the Institution as controller.
-

§ 11. Automated decision-making

The Platform does not make decisions based solely on automated processing, including profiling, which would produce legal effects concerning data subjects or similarly significantly affect them.

§ 12. Changes to the Privacy Policy

1. ZUBEL.PRO reserves the right to update this Privacy Policy in order to reflect changes in data processing practices, changes in the law or changes in the functionality of the Platform.
2. Users will be notified of material changes via the Platform or by e-mail at least **14 days** before the changes take effect.
3. Use of the Platform after the changes take effect constitutes acceptance of the updated Privacy Policy.

4. Each version of the Privacy Policy is published at a separate, permanent address (e.g. monteflow.cloud/privacy/1.3/); previous versions remain available at their addresses.

§ 13. Contact

For matters relating to the protection of personal data, please contact:

ZUBEL.PRO Krystian Zubel

ul. Orzechowa 5, 55-040 Dobkowice

E-mail: privacy@monteflow.cloud

We respond without undue delay, and no later than within 30 days.