

AUFTRAGSVERARBEITUNGSVERTRAG

Version: 1.3

Gültig ab: 01.11.2026

Ersetzt: Version 1.2 vom 21.07.2026

Verbindliches polnisches Original: <https://monteflow.cloud/dpa/1.3/>

Maschinelle Übersetzung — nur zur Information. Dieses Dokument ist eine maschinelle Übersetzung des polnischen Originals. Verbindlich ist ausschließlich die polnische Fassung; bei Abweichungen gilt der polnische Text.

Dieser Vertrag (nachfolgend: „**DPA**“) ist integraler Bestandteil des zwischen den Parteien geschlossenen Vertrags über die Erbringung des Dienstes MonteFlow.cloud (nachfolgend: „**Hauptvertrag**“), d. h.:

- eines über die Website im Wege der Akzeptanz der Nutzungsbedingungen von MonteFlow.cloud für Einrichtungen (nachfolgend: „**Nutzungsbedingungen**“) und der Leistung der Zahlung geschlossenen Vertrags („**Self-Service-Kauf**“), oder
- des Vertrags über die Erbringung des Dienstes MonteFlow.cloud oder eines anderen individuell mit dem Auftragsverarbeiter geschlossenen Vertrags („**Individualvertrag**“).

Der Abschluss des Hauptvertrags ist gleichbedeutend mit dem Abschluss des DPA und erfordert keine gesonderte Unterschrift (§ 14).

§ 1. Vertragsparteien

1. Verantwortlicher (Auftraggeber):

Verantwortlicher ist die **Einrichtung** — der Rechtsträger, der den Hauptvertrag geschlossen hat: - im Falle eines Individualvertrags — der in diesem Vertrag als „Einrichtung“ bezeichnete Rechtsträger, mit den dort angegebenen Identifikations-, Anschrifts- und Kontaktdaten sowie der dort benannten vertretungsberechtigten Person, - im Falle eines Self-Service-Kaufs — der durch die beim Kauf angegebenen Daten (Name, Anschrift des Sitzes, Steueridentifikationsnummer) bezeichnete Rechtsträger, dessen Kontaktadresse die E-Mail-Adresse des Inhaberkontos im Sinne der Nutzungsbedingungen ist.

Nachfolgend: „**Verantwortlicher**“ oder „**Einrichtung**“

2. Auftragsverarbeiter (Auftragnehmer):

Name: ZUBEL.PRO Krystian Zubel

Rechtsform: Einzelunternehmen

Anschrift des Sitzes: ul. Orzechowa 5, 55-040 Dobkowice, Polen

NIP (polnische Steuernummer): 913-153-70-18

Inhaber: Krystian Zubel

Kontakt – allgemeine Angelegenheiten: support@monteflow.cloud

Kontakt – Datenschutz: privacy@monteflow.cloud

Nachfolgend: „Auftragsverarbeiter“ oder „ZUBEL.PRO“

§ 2. Gegenstand und Umfang des Vertrags

1. Dieser Vertrag regelt die Bedingungen der Auftragsverarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß Art. 28 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachfolgend: „DSGVO“).
 2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, im Umfang und zum Zweck der Erbringung des Dienstes der Plattform **MonteFlow.cloud** (nachfolgend: „Dienst“ oder „Plattform“).
 3. Als dokumentierte Weisungen des Verantwortlichen gelten insbesondere: die Bestimmungen dieses Vertrags, die vom Verantwortlichen in der Plattform vorgenommenen Einstellungen (einschließlich der Wahl des Betriebsmodus: Basismodus oder Modus Compliance PL) sowie gesonderte schriftliche Anweisungen, die an die Adresse privacy@monteflow.cloud übermittelt werden.
 4. Bei Abweichungen zwischen den Dokumenten gilt die im Individualvertrag festgelegte Rangfolge, in dessen Ermangelung die in § 19 Abs. 2 der Nutzungsbedingungen festgelegte.
 5. Hat der Verantwortliche seinen Sitz außerhalb des Europäischen Wirtschaftsraums, werden die Daten vom Auftragsverarbeiter in der Europäischen Union gemäß diesem Vertrag und der DSGVO verarbeitet. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung nach dem für seinen Sitz maßgeblichen Recht verantwortlich, einschließlich der Übermittlung von Daten, die er selbst aus der Plattform exportiert. Soweit die Vorschriften des Kapitels V DSGVO dies erfordern, finden auf die Übermittlung von Daten durch den Auftragsverarbeiter an den Verantwortlichen die mit dem Durchführungsbeschluss (EU) 2021/914 der Kommission angenommenen Standardvertragsklauseln (Modul vier: Übermittlung vom Auftragsverarbeiter an den Verantwortlichen) Anwendung, welche die Parteien als in diesen Vertrag einbezogen betrachten.
-

§ 3. Einzelheiten der Verarbeitung

1. Gegenstand und Art der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit der Erbringung des Dienstes, der Folgendes umfasst: die Speicherung der vom Verantwortlichen und von den Nutzern der Plattform eingegebenen Daten, die Bereitstellung der Daten für berechtigte Nutzer, die Erstellung von Sicherungskopien, die Gewährleistung der Kontinuität

und Sicherheit des Dienstes sowie im Modus Compliance PL die Erstellung der nach den Vorschriften des Schulrechts erforderlichen Dokumentation.

2. Dauer der Verarbeitung

Die Verarbeitung dauert für die Laufzeit des Hauptvertrags an, unter Berücksichtigung der in § 9 festgelegten Übergangszeiträume.

3. Kategorien betroffener Personen

Der Auftragsverarbeiter verarbeitet Daten der folgenden Kategorien von Personen:

- Teilnehmer an von der Einrichtung durchgeführten Aktivitäten (Zöglinge, Schüler, Schulungsteilnehmer), einschließlich Kindern,
- Eltern und gesetzliche Vormünder der Kinder,
- Lehrkräfte, Personal und Mitwirkende der Einrichtung.

4. Kategorien verarbeiteter personenbezogener Daten

Daten der Teilnehmer (Zöglinge, Schüler, Schulungsteilnehmer, einschließlich Kinder):

- Vor- und Nachname,
- Geburtsdatum,
- Bildnis (Fotos — sofern von der Einrichtung eingegeben),
- pädagogische Beobachtungen,
- Informationen zur Anwesenheit,
- Daten zu Fähigkeiten und Fortschritten,
- Allergene und andere Gesundheitsdaten (sofern von der Einrichtung eingegeben),
- andere von der Einrichtung freiwillig eingegebene Daten.

Daten der Eltern/gesetzlichen Vormünder:

- Vor- und Nachname,
- E-Mail-Adresse,
- Telefonnummer,
- Nummer des Ausweisdokuments,
- Authentifizierungsdaten (Kontokennung),
- andere von der Einrichtung freiwillig eingegebene Daten.

Daten der Lehrkräfte und des Personals der Einrichtung:

- Vor- und Nachname,
- E-Mail-Adresse,
- Authentifizierungsdaten (Kontokennung),
- Informationen zur Rolle/Position in der Einrichtung.

Daten aus Audit-Protokollen (audit trail): - Kennung des Nutzers, der den Vorgang ausführt, - Art des Vorgangs (Lesen, Schreiben, Änderung, Löschung), - Datum und Uhrzeit des Vorgangs, - Kennung des Objekts, auf das sich der Vorgang bezog (z. B. Kennung des Kindes, der Beobachtung).

5. Besondere Kategorien von Daten (Art. 9 DSGVO)

1. Die Plattform ermöglicht dem Verantwortlichen die Eingabe von Gesundheitsdaten von Kindern (insbesondere Informationen über Allergene und Gesundheitszustände). Diese Daten sind besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO.
2. Der Verantwortliche ist allein dafür verantwortlich, über eine geeignete Rechtsgrundlage für die Verarbeitung besonderer Kategorien von Daten zu verfügen (insbesondere die ausdrückliche Einwilligung eines Elternteils/gesetzlichen Vormunds oder die Erfüllung rechtlicher Pflichten der Einrichtung).
3. Der Auftragsverarbeiter wendet auf besondere Kategorien von Daten dieselben Schutzmaßnahmen an wie auf die übrigen Daten, insbesondere Verschlüsselung, rollenbasierte Zugriffskontrolle sowie Datenisolierung zwischen Einrichtungen.
4. Der Auftragsverarbeiter wendet auf besondere Kategorien von Daten eine restriktive Zugriffskontrolle an, die den Zugriff auf diese Daten nur Nutzern mit Schuladministrator-Zugriff sowie Lehrkräften gestattet, die den Gruppen oder Kursen zugeordnet sind, die das Kind besucht. Der Schuladministrator kann anderen Konten über die Plattform ausdrücklich Zugriff auf diese Daten gewähren.

§ 4. Zweck der Verarbeitung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zu folgenden Zwecken:
 - Erbringung des Dienstes der Plattform MonteFlow.cloud,
 - Aufrechterhaltung der Sicherheit und Betriebskontinuität des Systems,
 - Erstellung und Aufbewahrung von Sicherungskopien,
 - Behebung technischer Probleme, die vom Verantwortlichen oder von Nutzern gemeldet werden,
 - Führung von Audit-Protokollen, die Vorgänge mit personenbezogenen Daten dokumentieren, um die Rechenschaftspflicht und die Sicherheit der Verarbeitung zu gewährleisten (Art. 5 Abs. 2 sowie Art. 32 DSGVO),
 - im Modus Compliance PL — Erstellung der nach den Vorschriften des Schulrechts erforderlichen Dokumentation auf Weisung des Verantwortlichen.
2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nicht für eigene Zwecke; insbesondere verwendet er die Daten nicht für Profiling, Analytik, Marketing, künstliche Intelligenz oder die Weitergabe an Dritte.

3. Der Verantwortliche ist allein dafür verantwortlich, über eine geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten (Art. 6 und Art. 9 DSGVO) zu verfügen, sowie für die Vereinbarkeit der Verarbeitung mit den Vorschriften des Schulrechts.
 4. Im Modus Compliance PL können die Vorschriften des Schulrechts zusätzliche Zwecke und Aufbewahrungsfristen für die Schuldokumentation festlegen. Der Verantwortliche ist für die Festlegung dieser Zwecke und Fristen verantwortlich, und der Auftragsverarbeiter setzt sie auf dessen dokumentierte Weisung um.
-

§ 5. Pflichten des Auftragsverarbeiters

1. Allgemeine Pflichten

1. Der Auftragsverarbeiter verpflichtet sich:
 - personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, es sei denn, die Pflicht zur Verarbeitung ergibt sich aus dem Unionsrecht oder dem polnischen Recht — in diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese Pflicht vor Beginn der Verarbeitung mit (sofern das Recht dies nicht verbietet),
 - zu gewährleisten, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben,
 - die in Anlage A festgelegten geeigneten technischen und organisatorischen Maßnahmen umzusetzen,
 - die in § 7 festgelegten Bedingungen für die Inanspruchnahme von Unterauftragsverarbeitern einzuhalten,
 - den Verantwortlichen bei der Erfüllung seiner Pflichten gegenüber den betroffenen Personen (Art. 15–22 DSGVO) zu unterstützen,
 - den Verantwortlichen bei der Erfüllung der in Art. 32–36 DSGVO festgelegten Pflichten (Sicherheit, Meldung von Verletzungen, Folgenabschätzung) zu unterstützen,
 - nach Beendigung der Erbringung des Dienstes die Daten gemäß § 9 zu löschen oder zurückzugeben,
 - dem Verantwortlichen die zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlichen Informationen zur Verfügung zu stellen.
2. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn eine Weisung des Verantwortlichen nach seiner Auffassung gegen die DSGVO oder andere Datenschutzvorschriften verstößt (Art. 28 Abs. 3 Unterabs. 2 DSGVO).

2. Datensicherheit

1. Der Auftragsverarbeiter hat die in Anlage A ausführlich beschriebenen technischen und organisatorischen Maßnahmen umgesetzt und hält sie aufrecht; sie gewährleisten ein dem mit der Verarbeitung verbundenen Risiko angemessenes Schutzniveau.

2. Der Auftragsverarbeiter verpflichtet sich zur regelmäßigen Überprüfung und Aktualisierung der angewandten Sicherheitsmaßnahmen, um deren Angemessenheit angesichts sich ändernder Bedrohungen zu gewährleisten.
3. Der Auftragsverarbeiter informiert den Verantwortlichen über wesentliche Änderungen der angewandten Sicherheitsmaßnahmen mindestens 14 Tage im Voraus.

3. Unterstützung bei den Rechten der betroffenen Personen

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung bei der Erfüllung der Pflichten aus Art. 15–22 DSGVO, insbesondere durch die Bereitstellung von Werkzeugen der Plattform, die den Export, die Änderung und die Löschung von Daten ermöglichen.
2. Der Auftragsverarbeiter leitet dem Verantwortlichen unverzüglich alle unmittelbar an den Auftragsverarbeiter gerichteten Anträge betroffener Personen weiter, ohne solche Anträge selbst zu beantworten.
3. Der Verantwortliche ist für die Bearbeitung der Anträge betroffener Personen sowie für deren Beantwortung innerhalb der von der DSGVO vorgeschriebenen Fristen verantwortlich.

§ 6. Pflichten des Verantwortlichen

1. Der Verantwortliche verpflichtet sich:
 - über eine geeignete Rechtsgrundlage für die Verarbeitung der dem Auftragsverarbeiter anvertrauten personenbezogenen Daten zu verfügen,
 - die betroffenen Personen über die Verarbeitung ihrer Daten in der Plattform zu informieren,
 - dem Auftragsverarbeiter ausschließlich datenschutzkonforme Weisungen zu erteilen,
 - den Auftragsverarbeiter unverzüglich über alle Änderungen des Umfangs oder des Zwecks der Verarbeitung zu benachrichtigen,
 - für die Sicherheit der Zugangsdaten zur Plattform zu sorgen (insbesondere der Anmeldedaten der Nutzer der Einrichtung),
 - Anträge und Beschwerden betroffener Personen zu bearbeiten.
2. Der Verantwortliche ist allein für die Rechtmäßigkeit der Datenverarbeitung (DSGVO, Schulrecht, andere einschlägige Vorschriften) verantwortlich, einschließlich der Einholung der erforderlichen Einwilligungen.

§ 7. Unterauftragsverarbeiter (weitere Auftragsverarbeitung)

1. Allgemeine Genehmigung und Liste der Unterauftragsverarbeiter

1. Der Verantwortliche erteilt eine allgemeine Genehmigung für die Inanspruchnahme der in Anlage B zu diesem Vertrag aufgeführten Unterauftragsverarbeiter durch den

Auftragsverarbeiter.

2. Identitätsanbieter, die beim optionalen Social Login (Apple, Google) genutzt werden, sind keine Unterauftragsverarbeiter im Sinne dieses Vertrags. Wählt der Nutzer diese Anmeldeart, authentifiziert er sich mit seinem eigenen Konto beim Anbieter, der die Daten als unabhängiger Verantwortlicher auf Grundlage eigener Bedingungen verarbeitet. Der Auftragsverarbeiter überträgt diesen Stellen keine unter diesen Vertrag fallenden Daten.
3. Zum Zeitpunkt des Vertragsschlusses nimmt der Auftragsverarbeiter folgende Unterauftragsverarbeiter in Anspruch:

Unterauftragsverarbeiter	Sitz	Datenstandort	Funktion	Übermittlungsgrundlage
Amazon Web Services EMEA SARL	Luxemburg (EU)	Server in der EU (eu-north-1 - Stockholm, Schweden; eu-south-1 - Mailand, Italien)	Hosting, Datenspeicherung, Cloud-Infrastruktur	Verarbeitung im EWR; AWS Inc. (USA) als Unter-Unterauftragsverarbeiter, der dem EU-US Data Privacy Framework unterliegt
Apple Distribution International Ltd	Cork, Irland (EU)	APNs-Infrastruktur (EU/USA)	Zustellung von Push-Benachrichtigungen an die mobile iOS-App — sofern die mobile iOS-App mit Push-Benachrichtigungen verfügbar ist	Verarbeitung im EWR; Apple Inc. (USA) als Unter-Unterauftragsverarbeiter, der dem EU-US Data Privacy Framework unterliegt
Google Cloud EMEA Limited	Dublin, Irland (EU)	FCM-Infrastruktur (EU/USA)	Zustellung von Push-Benachrichtigungen an die mobile Android-App — sofern die mobile Android-App mit Push-Benachrichtigungen verfügbar ist	Verarbeitung im EWR; Google LLC (USA) als Unter-Unterauftragsverarbeiter, der dem EU-US Data Privacy Framework unterliegt

Die mobile App befindet sich in der Testphase; ihre Bereitstellung für Nutzer ist für das Jahr 2026 geplant. Der Inhalt von Push-Benachrichtigungen wird minimiert — er enthält weder Gesundheitsdaten noch andere besondere Kategorien von Daten.

2. Verfahren bei Änderung von Unterauftragsverarbeitern

1. Der Auftragsverarbeiter informiert den Verantwortlichen über die beabsichtigte Hinzuziehung eines neuen Unterauftragsverarbeiters oder die Ersetzung eines bestehenden mindestens **30 Tage** im Voraus per E-Mail an die Kontaktadresse des Verantwortlichen (§ 1 Abs. 1).

2. Der Verantwortliche kann innerhalb von **14 Tagen** nach Erhalt der Benachrichtigung begründeten Widerspruch gegen den neuen Unterauftragsverarbeiter erheben.
 3. Im Falle eines Widerspruchs unternimmt der Auftragsverarbeiter angemessene Anstrengungen, um eine alternative Lösung vorzuschlagen. Erzielen die Parteien innerhalb von 30 Tagen nach Erhebung des Widerspruchs keine Einigung, ist der Verantwortliche berechtigt, den Hauptvertrag mit sofortiger Wirkung zu kündigen.
 4. Der Auftragsverarbeiter stellt sicher, dass jeder Unterauftragsverarbeiter an Datenschutzpflichten gebunden ist, die nicht geringer sind als die in diesem Vertrag festgelegten.
-

§ 8. Verletzungen des Schutzes personenbezogener Daten

1. Im Falle der Feststellung einer Verletzung des Schutzes personenbezogener Daten (Art. 33–34 DSGVO) benachrichtigt der Auftragsverarbeiter den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **36 Stunden** nach Feststellung der Verletzung, und übermittelt mindestens folgende Informationen:
 - eine Beschreibung der Art der Verletzung,
 - die Kategorien und die ungefähre Zahl der betroffenen Personen,
 - die voraussichtlichen Folgen der Verletzung,
 - eine Beschreibung der ergriffenen oder vorgeschlagenen Abhilfemaßnahmen.
 2. Sind zum Zeitpunkt der ersten Benachrichtigung nicht alle Informationen verfügbar, übermittelt der Auftragsverarbeiter sie schrittweise ohne unnötige Verzögerung.
 3. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Pflichten zur Meldung der Verletzung an die Aufsichtsbehörde (polnische Datenschutzbehörde, UODO) sowie zur Benachrichtigung der betroffenen Personen.
 4. Der Auftragsverarbeiter dokumentiert alle Verletzungen des Schutzes personenbezogener Daten, einschließlich der Umstände der Verletzung, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen.
-

§ 9. Löschung und Rückgabe der Daten nach Vertragsende

1. Nach Beendigung des Hauptvertrags und Ablauf der Gültigkeit der Lizenz gewährt der Auftragsverarbeiter dem Verantwortlichen einen 30-tägigen Zugang im Nur-Lese-Modus (read-only), der den Datenexport ermöglicht. Die Gültigkeit der Lizenz nach Beendigung des Hauptvertrags bestimmen die Nutzungsbedingungen (§ 12 Abs. 1) oder der Individualvertrag.
2. Nach Ablauf des Nur-Lese-Zeitraums verfährt der Auftragsverarbeiter auf Weisung des Verantwortlichen ohne unnötige Verzögerung wie folgt:
 - er gibt alle personenbezogenen Daten in einem strukturierten Format (CSV, JSON oder XML) zurück, oder

- er löscht alle personenbezogenen Daten von den Produktionsservern.
3. Liegt innerhalb von 30 Tagen nach Ende des Nur-Lese-Zeitraums keine ausdrückliche Weisung des Verantwortlichen vor, löscht der Auftragsverarbeiter alle personenbezogenen Daten von den Produktionsservern. Auf schriftliche Weisung des Verantwortlichen kann die Löschung früher erfolgen, auch vor Ablauf des Nur-Lese-Zeitraums.
 4. Daten in Sicherungskopien werden gemäß dem Rotationszyklus der Sicherungskopien innerhalb von bis zu **90 Tagen** nach der Löschung aus dem Produktivsystem automatisch gelöscht.
 5. **Nach der Löschung aufbewahrte Daten.** Bei der Löschung von Daten gemäß Abs. 2 oder 3 bewahrt der Auftragsverarbeiter ausschließlich Folgendes auf:
 1. **ein Archiv des vollständigen Datenexports — ausschließlich für Verantwortliche, die den Modus Compliance PL nutzen.** Das Archiv wird vor der Löschung jeglicher Daten erstellt und verifiziert, für **90 Tage** ab der Löschung ausschließlich zum Zweck seiner Rückgabe an den Verantwortlichen auf Verlangen (Abs. 2) aufbewahrt und anschließend automatisch gelöscht. Für Verantwortliche, die den Modus Compliance PL nicht nutzen, wird kein Archiv erstellt;
 2. **Abrechnungsdaten** — Lizenzen, Rechnungen und Korrekturrechnungen, vom Zahlungsdienstleister empfangene Ereignisse, Ergebnisse der Verifizierung von USt-IdNr. sowie Identifikationsdaten des Verantwortlichen für Abrechnungszwecke (Name, Steueridentifikationsnummer, Anschrift, E-Mail-Adresse für die Abrechnung, Zahlungs- und Rechnungskennungen). Diese Daten verarbeitet der Auftragsverarbeiter als Verantwortlicher gemäß der Datenschutzerklärung für 18 Monate; die nach den Steuervorschriften erforderliche Dokumentation wird in den in der Datenschutzerklärung genannten Rechnungs- und Zahlungssystemen aufbewahrt;
 3. **das Systemereignisprotokoll (Audit)** — bis zum Ablauf der Aufbewahrungsfrist der einzelnen Einträge; Einträge, welche die Erteilung von Berechtigungen, die Löschung von Daten auf Verlangen der betroffenen Person, die Erfassung der Gesundheitseinwilligung sowie die Löschung der Daten des Verantwortlichen selbst dokumentieren, werden 10 Jahre lang als Nachweis der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) aufbewahrt;
 4. **Sicherungskopien** — bis zu deren Ablauf gemäß Abs. 4.
 6. Nutzerkonten, die ausschließlich zum Verantwortlichen gehören, dessen Daten gelöscht werden, werden gelöscht. Ein Nutzer, der auch einer anderen Einrichtung angehört, welche die Plattform nutzt, behält sein Konto und verliert den Zugriff auf die Daten des Verantwortlichen; die Daten dieses Nutzers in Bezug auf die andere Einrichtung werden auf Weisung dieser Einrichtung als eigenständiger Verantwortlicher verarbeitet.
 7. Nach der Löschung der Daten übermittelt der Auftragsverarbeiter dem Verantwortlichen an die Kontaktadresse sowie an die E-Mail-Adresse für die Abrechnung eine Löschbestätigung mit Informationen über die gemäß Abs. 5 aufbewahrten Daten.
 8. Im Modus Compliance PL ist der Verantwortliche dafür verantwortlich, die nach den Vorschriften des Schulrechts erforderlichen Daten vor Ablauf des Nur-Lese-Zeitraums zu exportieren. Das in Abs. 5 Nr. 1 genannte Archiv ersetzt diese Pflicht nicht. Der

Auftragsverarbeiter haftet nicht für einen unterlassenen Datenexport durch den Verantwortlichen.

9. Der Auftragsverarbeiter kann Daten aufbewahren, wenn das Unionsrecht oder das polnische Recht eine weitere Speicherung vorschreibt — in diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen über die Rechtsgrundlage einer solchen Speicherung.

§ 10. Audits und Inspektionen

1. Der Auftragsverarbeiter stellt dem Verantwortlichen die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlichen Informationen zur Verfügung und ermöglicht die Durchführung von Audits und Inspektionen.
2. Audits und Inspektionen finden unter folgenden Bedingungen statt:
 - der Verantwortliche kündigt die beabsichtigte Durchführung eines Audits mindestens **14 Tage** im Voraus an,
 - Audits werden während der Geschäftszeiten des Auftragsverarbeiters (Montag–Freitag, 9:00–17:00 Uhr) durchgeführt,
 - planmäßige Audits werden nicht häufiger als **einmal pro Kalenderjahr** durchgeführt, es sei denn, das Audit steht im Zusammenhang mit einer konkreten Verletzung des Schutzes personenbezogener Daten,
 - der Auditor ist zur Vertraulichkeit hinsichtlich der Daten anderer Kunden des Auftragsverarbeiters verpflichtet,
 - die Kosten des Audits trägt der Verantwortliche, es sei denn, das Audit ergibt eine wesentliche Verletzung der Pflichten des Auftragsverarbeiters.
3. Auf Wunsch des Verantwortlichen stellt der Auftragsverarbeiter die Dokumentation zu den in Anlage A beschriebenen angewandten Sicherheitsmaßnahmen zur Verfügung.

§ 11. Haftung

1. Die Haftung der Parteien für die Verletzung von Pflichten aus diesem Vertrag bestimmt sich nach den Vorschriften der DSGVO (insbesondere Art. 82) sowie nach dem polnischen Zivilgesetzbuch (Kodeks cywilny).
2. Der Auftragsverarbeiter haftet nicht für Verletzungen, die verursacht werden durch:
 - Handlungen oder Unterlassungen des Verantwortlichen, seiner Mitarbeiter oder der Nutzer der Plattform,
 - DSGVO-widrige Weisungen des Verantwortlichen, über die der Auftragsverarbeiter den Verantwortlichen gemäß § 5 Abs. 2 informiert hat,
 - einen unterlassenen Datenexport durch den Verantwortlichen innerhalb der in § 9 festgelegten Fristen.

3. Die Gesamthaftung des Auftragsverarbeiters auf Schadensersatz gegenüber dem Verantwortlichen aus diesem Vertrag ist auf einen Betrag begrenzt, der der Summe der vom Verantwortlichen an den Auftragsverarbeiter in den **12 Monaten** vor dem den Anspruch begründenden Ereignis entrichteten Gebühren entspricht. Diese Beschränkung gilt nicht für vorsätzlich verursachte Schäden und berührt keine zwingenden Rechtsvorschriften.
-

§ 12. Laufzeit und Vertragsänderungen

1. Der DPA tritt mit dem Tag des Abschlusses des Hauptvertrags in Kraft und gilt für dessen Laufzeit.
 2. Der Auftragsverarbeiter veröffentlicht jede neue Fassung des DPA unter einer gesonderten, festen Adresse und unterhält ein Archiv früherer Fassungen. Veröffentlichte Fassungen werden nicht geändert. Die Parteien sind an die gemäß § 14 Abs. 2 bestimmte Fassung gebunden, bis zu deren Änderung im Verfahren nach Abs. 3–5.
 3. Beabsichtigt der Auftragsverarbeiter Änderungen, welche die Bedingungen der Datenverarbeitung wesentlich beeinflussen, informiert er den Verantwortlichen per E-Mail an die Kontaktadresse (§ 1 Abs. 1) mindestens **30 Tage** im Voraus unter Angabe des Umfangs und der Begründung der Änderungen. Der Verantwortliche kann innerhalb von **14 Tagen** nach Erhalt der Benachrichtigung Widerspruch erheben. Erfolgt innerhalb dieser Frist kein Widerspruch, gelten die Änderungen als akzeptiert.
 4. Im Falle eines Widerspruchs nehmen die Parteien Verhandlungen auf; bis zu deren Abschluss sind die Parteien an die bisherige Fassung des DPA gebunden. Erzielen die Parteien innerhalb von 30 Tagen nach Erhebung des Widerspruchs keine Einigung, ist der Verantwortliche berechtigt, den Hauptvertrag mit sofortiger Wirkung zu kündigen, ohne hierfür zu haften.
 5. Andere als die in Abs. 3 genannten Änderungen — insbesondere redaktionelle Korrekturen, Aktualisierungen von Kontaktdaten sowie Änderungen, die sich aus Änderungen des allgemein geltenden Rechts ergeben — kann der Auftragsverarbeiter mit ihrer Veröffentlichung einführen, wobei er den Verantwortlichen bei der nächsten Benachrichtigung darüber informiert.
 6. Änderungen der Liste der Unterauftragsverarbeiter unterliegen ausschließlich dem in § 7 Abs. 2 festgelegten Verfahren.
 7. Die Pflichten des Auftragsverarbeiters in Bezug auf Vertraulichkeit und Datensicherheit gelten auch nach Beendigung des DPA fort.
-

§ 13. Schlussbestimmungen

1. **Vertraulichkeit:** Der Auftragsverarbeiter verpflichtet sich, alle vom Verantwortlichen erhaltenen Informationen, einschließlich des Inhalts der verarbeiteten personenbezogenen Daten, vertraulich zu behandeln. Die Vertraulichkeitspflicht ist zeitlich unbegrenzt.
2. **Anwendbares Recht:** Der Vertrag unterliegt polnischem Recht.

3. **Streitbeilegung:** Alle Streitigkeiten aus dem Vertrag werden die Parteien gütlich beizulegen versuchen. Kommt keine Einigung zustande, werden die Streitigkeiten von dem für den Sitz des Auftragsverarbeiters zuständigen ordentlichen Gericht entschieden.
 4. **Salvatorische Klausel:** Sollte eine Bestimmung des Vertrags für nichtig oder unwirksam befunden werden, bleiben die übrigen Bestimmungen wirksam. Die Parteien ersetzen die nichtige Bestimmung durch eine Bestimmung, die dem wirtschaftlichen Zweck der nichtigen Bestimmung am nächsten kommt.
 5. Dieser Vertrag bildet zusammen mit den Anlagen die gesamte Vereinbarung der Parteien über die Auftragsverarbeitung personenbezogener Daten und ersetzt alle früheren diesbezüglichen Absprachen.
-

§ 14. Abschluss des DPA

1. Dieser DPA wird zusammen mit dem Hauptvertrag geschlossen und erfordert keine gesonderten Unterschriften der Parteien; die elektronische Form ist ausreichend (Art. 28 Abs. 9 DSGVO):
 - im Falle eines Self-Service-Kaufs — mit dem Zeitpunkt des Vertragsschlusses gemäß den Nutzungsbedingungen, nach Akzeptanz der Nutzungsbedingungen, die den Abschluss des DPA vorsehen,
 - im Falle eines Individualvertrags — mit dem Zeitpunkt seines Abschlusses.
 2. Die Parteien sind an folgende Fassung des DPA gebunden:
 - im Falle eines Self-Service-Kaufs — die zum Zeitpunkt der Akzeptanz der Nutzungsbedingungen als aktuelle Version veröffentlichte, auch wenn sie gegenüber Verantwortlichen, die den Hauptvertrag früher geschlossen haben, gemäß § 12 Abs. 3 zu einem späteren Zeitpunkt in Kraft tritt; der Auftragsverarbeiter erfasst das Datum der Akzeptanz und die Version des DPA und übersendet dem Verantwortlichen eine Bestätigung mit einem Link zu dieser Fassung,
 - im Falle eines Individualvertrags — die in diesem Vertrag angegebene,und in jedem Fall — eine später im Verfahren nach § 12 Abs. 3–5 eingeführte Fassung.
-

ANLAGE A: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

A.1. Technische Maßnahmen

- Verschlüsselung von Daten bei der Übertragung (TLS 1.2+).
- Verschlüsselung ruhender Daten (AES-256, von AWS verwaltet).
- Georedundante Datenspeicherung (mindestens 2 Verfügbarkeitszonen in der EU-Region).
- Tägliche automatische Sicherungskopien mit einer Aufbewahrungsdauer von bis zu 90 Tagen.

- Rollenbasierte Zugriffskontrolle (RBAC) nach dem Prinzip der minimalen Berechtigungen.
- Protokollierung und Überwachung von Datenzugriffen und Systemänderungen (audit trail).
- Multi-Faktor-Authentifizierung (MFA) für Administratorkonten.
- Isolierung der Daten verschiedener Einrichtungen auf Datenbankebene (tenant isolation).
- Von AWS bereitgestellter Infrastrukturschutz (Firewall, DDoS-Schutz, physische Sicherung der Rechenzentren).
- Regelmäßige Aktualisierungen von Software und Abhängigkeiten.

A.2. Organisatorische Maßnahmen

- Prinzip der minimalen Berechtigungen — Zugang zu personenbezogenen Daten haben ausschließlich Personen, für die dies zur Erbringung des Dienstes erforderlich ist.
- Vertraulichkeitsverpflichtungen aller Personen mit Zugang zu den Daten.
- Verfahren zur Zugriffsverwaltung (Erteilung und Entzug von Berechtigungen).
- Verfahren zur Behandlung von Sicherheitsvorfällen.
- Verfahren zur Erstellung, Überprüfung und Wiederherstellung von Sicherungskopien.
- Verfahren zur Bearbeitung von Anträgen betroffener Personen.
- Regelmäßige Überprüfungen der angewandten Sicherheitsmaßnahmen.

A.3. Ort der Verarbeitung

Alle personenbezogenen Daten werden auf AWS-Servern in der Europäischen Union gespeichert und verarbeitet:

- **Primäre Region:** eu-north-1 (Stockholm, Schweden)
- **Ausweichregion:** eu-south-1 (Mailand, Italien)

ANLAGE B: LISTE DER UNTERAUFTRAGSVERARBEITER

Unterauftragsverarbeiter	Sitz	Datenstandort	Funktion	Übermittlungsgrundlage (falls außerhalb des EWR)
Amazon Web Services EMEA SARL	Luxemburg (EU)	eu-north-1, eu-south-1 (EU)	Hosting, Rechenleistung, Datenspeicherung, Cloud-Infrastruktur (Lambda, DynamoDB, S3, CloudFront, Cognito, API Gateway, SNS)	Verarbeitung im EWR. AWS Inc. (USA) als Unter- Unterauftragsverarbeiter: EU-US Data Privacy Framework

Unterauftragsverarbeiter	Sitz	Datenstandort	Funktion	Übermittlungsgrundlage (falls außerhalb des EWR)
Apple Distribution International Ltd	Cork, Irland (EU)	APNs-Infrastruktur (EU/USA)	Zustellung von Push-Benachrichtigungen an die mobile iOS-App — sofern die mobile iOS-App mit Push-Benachrichtigungen verfügbar ist	Verarbeitung im EWR. Apple Inc. (USA) als Unter-Unterauftragsverarbeiter: EU-US Data Privacy Framework
Google Cloud EMEA Limited	Dublin, Irland (EU)	FCM-Infrastruktur (EU/USA)	Zustellung von Push-Benachrichtigungen an die mobile Android-App — sofern die mobile Android-App mit Push-Benachrichtigungen verfügbar ist	Verarbeitung im EWR. Google LLC (USA) als Unter-Unterauftragsverarbeiter: EU-US Data Privacy Framework

Die mobile App befindet sich in der Testphase; ihre Bereitstellung für Nutzer ist für das Jahr 2026 geplant. Der Inhalt von Push-Benachrichtigungen wird minimiert — er enthält weder Gesundheitsdaten noch andere besondere Kategorien von Daten.

Identitätsanbieter, die beim optionalen Social Login (Apple, Google) genutzt werden, sind keine Unterauftragsverarbeiter — sie verarbeiten Daten als unabhängige Verantwortliche gemäß § 7 Abs. 1 Nr. 2.

Der Verantwortliche genehmigt die oben aufgeführten Unterauftragsverarbeiter mit dem Tag des Abschlusses dieses Vertrags. Änderungen der Liste der Unterauftragsverarbeiter unterliegen dem in § 7.2 festgelegten Verfahren.

Version: 1.3 · Gültig ab: 01.11.2026 · Ersetzt: Version 1.2 vom 21.07.2026

ZUBEL.PRO Krystian Zubel

ul. Orzechowa 5, 55-040 Dobkowice

NIP: 913-153-70-18

support@monteflow.cloud | privacy@monteflow.cloud