Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 EU Datenschutz-Grundverordnung

Der Verantwortliche:	Der Auftragsverarbeiter:
_____	Limitis GmbH
_____	St. Margarethenplatz 2
_____	39035 Welsberg – Italien
_____	MwSt.-Nr. 02548890215
_____	
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

- Web-Hosting und Server-Hosting auf den firmeneigenen Servern des Auftragnehmers, um diese den Kunden über das Internet zur Verfügung zu stellen.
- E-Mail-Dienste und Pec-Postfächer
- WLAN Dienste
- Domainregistrierung
- Housing
- Office 365
- Backup und Cloud-Dienste
- Durchführen von Wartungs- und Supporttätigkeiten für die vom Auftragnehmer verwalteten Dienste zur Aufrechterhaltung der Zugriffssicherheit, der Datensicherheit und Sicherheit in Bezug auf Angriffe von außen.
- Betrieb, Wartungs- und Supporttätigkeit der Web Applikation „Digitales Register“ auf den firmeneigenen Servern des Auftragnehmers, um diese den Kunden über das Internet zur Verfügung zu stellen.

Diese Vereinbarung ist als Ergänzung zur Beauftragung, welcher zwischen Auftraggeber und Auftragnehmer abgeschlossen wurde, zu verstehen.

Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

a) Art der Daten laut Art. 4 Abs. 1, 13, 14,15 DS-GVO

Familienname, Vorname, Firmenbezeichnung, vollständige Adresse, Steuernummer, Mehrwertsteuernummer, E-Mail-Adresse, Logfiles, technische Protokolldaten, Benutzername, Personenrolle, Status Benutzerzugang, Sprache, letzte Anmeldung, Passwort, Google Authenticator Schlüssel

Nur für den Dienst „Digitales Register“: Foto, Geburtsdatum, Klasse, Alter, Abwesenheiten, Stundenplan, Noten, Beobachtungen, Befreiungen, Klassenvorstand der Klassen,

b) Kreis der Betroffenen laut Art. 4 Abs.1 DS-GVO

Kunden des Auftraggebers und deren Mitarbeiter
Für das Digitale Register: Schüler, Eltern, Lehrer

c) Art der Verarbeitung laut Art. 4 Abs. 2 DS-GVO

Es erfolgt eine Speicherung dieser Daten. Im Rahmen des Hostings und Betriebs ist ein Zugriff auf diese Daten nicht ausgeschlossen. Möglicherweise erfolgt dabei bedarfsorientiert eine Anpassung oder Veränderung, ein Auslesen, Abfragen, eine Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung oder der Abgleich dieser Daten.

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien unter Einhaltung der Vertragsdauer und der definierten Kündigungsfrist gekündigt werden.

3. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für andere oder für eigene Zwecke des Auftragnehmers einer schriftlichen Genehmigung.
(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat, oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ergriffen hat und ermöglicht diesbezüglich auch Prüfungen durch den Auftraggeber (weitere Informationen sind der Anlage 1 zu entnehmen).

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(4) Der Auftragnehmer ergreift technische und organisatorische Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die personenbezogene Daten enthalten, im Auftrag des Auftraggebers zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

4. MITTEILUNGSPFLICHTEN DES AUFTRAGNEHMERS BEI STÖRUNGEN DER VERARBEITUNG UND BEI VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten angemessen zu unterstützen.

5. PFLICHTEN DES AUFTRAGGEBERS

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

6. WEISUNGSBERECHTIGTE DES AUFTRAGGEBERS, WEISUNGSEMPFÄNGER DES AUFTRAGNEHMERS

Weisungsberechtigte Personen des Auftraggebers sind:

_____
(Vorname, Name, Organisationseinheit, E-Mail-Adresse)

_____
(Vorname, Name, Organisationseinheit, E-Mail-Adresse)

_____
(Vorname, Name, Organisationseinheit, E-Mail-Adresse)

_____
(Vorname, Name, Organisationseinheit, E-Mail-Adresse)

_____
(Vorname, Name, Organisationseinheit, E-Mail-Adresse)

Weisungsempfänger beim Auftragnehmer sind:

Philipp Moser, Limitis GmbH, info@limitis.com
Markus Gufler, Limitis GmbH, support@limitis.com
Digitales Register: Stefan Raffeiner (UNTIS), Alexander Trojer, support@digitalesregister.it

Für Weisung zu nutzende Kommunikationskanäle:
E-Mail: privacy@limitis.com

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

7. ORT DER DURCHFÜHRUNG DER DATEN-VERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

8. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen (nur für den Service „Digitales Register“):

Untis GmbH
Belvederegasse 11
2000 Stockerau – Österreich

Der Auftragnehmer Limitis GmbH, sowie der Sub-Auftragsverarbeiter Untis GmbH sind jeweils befugt folgende Personen als Sub-Auftragsverarbeiter hinzuzuziehen (nur für den Service „Digitales Register“):

Alex Trojer
Jaufenstrasse 4B
39019 Tirol – Italien

Stefan Raffeiner
Hellwagstrasse 21/54
1200 Wien - Österreich

Beabsichtigte Änderungen der bzw. des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies gegebenenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen.

_____, am _____

Für den Auftraggeber:

.....

[*Name samt Funktion*]

Welsberg, am 17.05.2018

Für den Auftragnehmer:

Firmato digitalmente da
PHILIPP MOSER
C = IT

.....

Philipp Moser, CEO
Limitis GmbH

Anlage 1 – Technisch-organisatorische Maßnahmen

.

1. VERTRAULICHKEIT

- **Zutrittskontrolle:**

Die Server für den Betrieb der Web Applikation sind im Rechenzentrum Brennercom „b.Cube“ Bozen untergebracht. Das Rechenzentrum gewährleistet die Zutrittskontrolle durch eine Zutrittskontroll- und Überwachungsanlage, eine Personenschleuse, eine Videoüberwachungsanlage und Wachpersonal. Es besteht ein mehrstufiges System zur Identifikation von zutrittsberechtigten Personen (ID-Karte, Fingerabdrucksprüfung).
Der physische Zutritt zu den Servern ist durch einen abgesperrten Serverschrank im zugangskontrollierten Gebäude gegeben. Die Schlüsselvergabe ist genau geregelt und auf die notwendigen Personen beschränkt.

- **Zugangskontrolle**:

Nur ausgewählte und an das jeweilige Rechenzentrum genannte Mitarbeiter haben Zugang zu den Servern, auf welchen die Web Applikation betrieben wird. Diese Server werden daher auch ausschließlich von Mitarbeitern von Limitis GmbH betreut und gewartet.
Die Serversysteme sind über das Internet ausschließlich über einen verschlüsselten SSH-Zugang zu erreichen. Die Authentifizierung erfolgt über Zertifikate, die dem derzeitigen Stand der Technik entsprechen und laufend dem aktuellen Stand der Technik angepasst wird.

- **Zugriffskontrolle**:

Die Web Applikation verfügt über passwortgeschützte Benutzerzugänge.
Das Berechtigungssystem ermöglicht Zugriffs- und Zuständigkeitsbeschränkungen.
Eine Firewall schützt die Server vor unbefugtem Zugriff.
Die Betreiber des Rechenzentrums haben keine Befugnis zum Zugriff auf die Server von Limitis.

- **Verarbeitungskontrolle:**

Sämtliche relevante Daten werden während der Verarbeitung durch entsprechende Protokolle bzw. Sicherheitsmaßnahme (z.B. Verschlüsselung, etc.) vor unberechtigtem Zugriff geschützt.

2. INTEGRITÄT

- **Weitergabekontrolle**:

Durch den Einsatz entsprechender Verschlüsselungskontrolle bzw. entsprechender Übertragungsprotokolle ist die Veränderung von Daten während des Transports bzw. bei der Speicherung und Verarbeitung ausgeschlossen.
Zur Gewährleistung der Weitergabekontrolle werden sämtliche personenbezogenen Daten während der Übermittlung in den genannten Fällen einer https-Verschlüsselung (nach dem Stand der Technik) unterzogen.

- **Eingabekontrolle**:

Die Veränderung personenbezogener Daten wird durch entsprechende Zugriffsbeschränkungen eingeschränkt, bzw. ist durch geeignete Maßnahmen nachvollziehbar.
Jede Anmeldung am System wird protokolliert und sämtliche zur Rückverfolgung erforderlichen Daten werden festgehalten. Erfolglose Anmeldungen werden ebenso erfasst. Sämtliche Änderungen an den Bewegungsdaten werden automatisch protokolliert. Dies beinhaltet sowohl die inhaltliche Änderung, als auch von wem die Änderung durchgeführt wurde.

3. VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**:
  Die Verfügbarkeit und Stabilität der Systeme ist durch technische und organisatorische Maßnahmen sichergestellt:
  - Backup-Strategie (online/offline; on-site/off-site)
  - Notfallplanung
  - Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
  - Firewall-Systeme nach aktuellem Stand der Technik
  - Distributed Denial of Service (DDoS) Schutz
  - Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

  Gespiegelte Festplatten im jeweiligen Server, Datenbankreplikation auf einen zweiten Server und tägliches Backup schützen die Daten vor zufälliger Zerstörung oder Verlust (siehe auch Punkt 4.1.).

- **Rasche Wiederherstellbarkeit:**
  Die rasche Widerherstellbarkeit wird durch entsprechende Segmentierung der Daten erreicht, wodurch bspw. im Fehlerfall nur die betroffenen Datenstände wiederhergestellt werden müssen.

- **Löschungsfristen**:
  Bei Beendigung der Zusammenarbeit werden die Daten nach spätestens 3 Monaten gelöscht, außer es gelten andere gesetzliche Bestimmungen.