Vertrag über die Auftragsverarbeitung personenbezogener Daten (AVV)

zwischen der Lets GmbH (im Folgenden: **Auftragnehmer**) und Unternehmenskunden (im Folgenden: **Auftraggeber**), die das Angebot der Lets GmbH auf der Plattform joinlets.de (im Folgenden: **Plattform**) nutzen.

1. Einleitung, Geltungsbereich, Definitionen
    a. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden: **Parteien**) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
    b. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer und dessen Mitarbeiter personenbezogene Daten im Auftrag des Auftraggebers verarbeiten.
    c. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“.

2. Gegenstand und Dauer der Verarbeitung
    a. Gegenstand

Der Auftragnehmer betreibt für den Auftraggeber eine Plattform, auf der sich Mitarbeiter des Auftraggebers im Rahmen nachhaltiger, ökologischer, ökonomischer und sozialer Projekte, die von Initiativen und Organisationen auf der Plattform angeboten oder von dem Auftraggeber veranstaltet werden, engagieren können.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertragsverhältnis, welches in den „Allgemeinen Geschäftsbedingungen für die lets Webplattform gegenüber Unternehmenskunden“ geregelt ist (im Folgenden: **Hauptvertrag**).

    b. Dauer

Die Verarbeitung beginnt mit Abschluss des Hauptvertrags und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

2. Art, Zweck und Betroffene der Datenverarbeitung:
    a. Art der Verarbeitung

Die Verarbeitung ist folgender Art: Der Auftragsverarbeiter verarbeitet personenbezogene Daten der Mitarbeiter des Auftraggebers, die sich auf der Plattform registrieren. Die Verarbeitung umfasst die Erhebung und Speicherung der von den Mitarbeitern angegebenen Daten zu ihrer Person, ihre Interaktion mit der Plattform und Beteiligung an Projekten sowie die Auswertung der Nutzung der Plattform.

    b. Zweck der Verarbeitung

Die Verarbeitung dient folgenden Zwecken: Erbringung der vertragsgegenständlichen Leistung zur Bereitstellung einer Webplattform, auf der sich Mitarbeiter des Auftraggebers im Rahmen nachhaltiger, ökologischer, ökonomischer und sozialer Projekte engagieren können, die von

Initiativen und Organisationen auf der Plattform angeboten oder von dem Auftraggeber veranstaltet werden.

c. Art der Daten

Es werden folgende Daten verarbeitet:

- Stammdaten (Name, Zugangsdaten, Geburtsdatum, E-Mail-Adresse, Unternehmenszugehörigkeit, ggf. Telefonnummer, Tätigkeitsbeschreibung,)
- Aktivitätsdaten (Projektteilnahme, Standort, Projektkommunikation, Text- und Bildbeiträge, Plattforminteraktion wie z.B. Folgen oder Liken, etc.)

d. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Mitarbeiter des Auftraggebers und dessen verbundener Unternehmen

4. Pflichten des Auftragnehmers

a. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

b. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

c. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

d. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung und dann regelmäßig mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden.

e. Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde.

f. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

g. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5. Sicherheit der Verarbeitung

Der Auftragnehmer ergreift die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten
    a. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
    b. Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7. Unterauftragsverhältnisse
    a. Der Auftragnehmer ist berechtigt, Unterauftragsverarbeiter einzusetzen. Derzeit eingesetzte Unterauftragsbearbeiter sind in Anlage 2 genannt.
    b. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Hinzuziehung oder Ersetzung eines (weiteren) Unterauftragsverarbeiters mindestens [14 Tage] vor der geplanten Hinzuziehung oder Ersetzung über diese in Kenntnis setzen. Widerspricht der Auftraggeber der Hinzuziehung oder Ersetzung innerhalb dieser Frist, und entscheidet der Auftraggeber, den jeweiligen Unterauftragsverarbeiter einzusetzen, steht dem Auftragnehmer das Recht zur außerordentlichen Kündigung zu.
    c. Nimmt der Auftragnehmer einen Unterauftragsverarbeiter in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragsverarbeiter im Wege einer AVV dieselben Datenschutzpflichten wie in dieser AVV auferlegt, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des anwendbaren Datenschutzrechts erfolgt. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

8. Rechte und Pflichten des Auftraggebers
    a. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
    b. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
    c. Der Auftraggeber ist berechtigt, die Einhaltung dieser AVV beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort (jeweils soweit erforderlich) zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

d. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

9. Mitteilungspflichten

a. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Die Mitteilung hat an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
    i. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
    ii. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
    iii. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
    iv. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
b. Der Auftragnehmer wird den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang unterstützen.

10. Weisungen

a. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
b. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. Beendigung des Auftrags

Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen; mangels Erklärung ist der Auftragnehmer berechtigt, die Daten oder Kopien zu vernichten.

Lets GmbH
Juli 2023

Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer einrichtet und aufrechterhält. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Da der Auftragnehmer den Betrieb der Internet-Dienstleistung auf joinlets.de ausschließlich auf der Infrastruktur des auf externes Server-Hosting spezialisierten Sub-Auftragsverarbeiters Amazon Web Services EMEA SARL (AWS) am Standort Frankfurt am Main betreibt und in den Räumlichkeiten des Auftragnehmers selbst keine personenbezogenen Daten von Nutzern gespeichert oder verarbeitet werden, beschränken sich die nachstehenden TOM auf die vom Auftragnehmer in seinen Räumlichkeiten gesetzten Sicherheitsmaßnahmen.

Informationen zu den TOM für das externe Server-Hosting sind hier abrufbar.

Der Auftragnehmer verschlüsselt sämtliche personenbezogenen Daten in der Internet-Dienstleistung joinlets.de mit Hilfe des AWS Key Management System sicher (256bit), so dass ein unberechtigter Zugriff auf diese Daten ausgeschlossen ist.

Darüber hinaus ergreift der Auftragnehmer folgende Maßnahmen:

1. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können:

Alle Systeme sind passwortgeschützt. Abgesicherter Zugang des Entwicklungs- und Verwaltungsbereichs mit einem Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge). Organisatorische Maßnahmen bei Beendigung eines Dienstverhältnisses mit einem Mitarbeiter (Zugang wird gelöscht). Einrichtung eines Benutzerstammsatzes pro Anwender. Die Übertragung von Daten erfolgt ausschließlich über eine per SSL verschlüsselte Verbindung.

2. Zugriffskontrolle

Es besteht eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

3. Weitergabekontrolle

Maßnahmen, dass personenbezogene Daten bei der elektronischen Übertragung oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können, und dass festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist. Der Austausch von personenbezogenen Daten erfolgt ausschließlich innerhalb der Systeme des Auftragnehmers sowie ggf. deren Sub-Auftragsverarbeiter. Zwischen den einzelnen Systemen werden die Daten entweder lokal oder über eine per SSL verschlüsselte Datenverbindung übertragen.

Personenbezogene Daten werden im Zuge der Weitergabe und Verarbeitung nicht verändert und bleiben unversehrt, vollständig und aktuell. Der Auftragnehmer unternimmt alles Notwendige, um zu verhindern, dass

Daten verfälscht werden oder falsche Daten verarbeitet werden. Gleichzeitig ist gewährleistet, dass Änderungen an Daten nachvollzogen werden können.

4. Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind. Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet und nur vom Teilnehmer, dem Auftraggeber (und dessen Anwendern) sowie durch den Anwender-Support von Lets erstellt und/oder bearbeitet werden. Jede Veränderung wird mit dem Nutzer sowie einem Zeitstempel dokumentiert. Darüber hinaus erfolgt die Protokollierung über Logfiles.

5. Auftragskontrolle

Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer. Dies bedeutet zunächst die eindeutige Vertragsgestaltung und formalisierte Auftragserteilung (Auftragsbestätigung). Der Auftragnehmer gewährleistet durch die nachstehenden Maßnahmen, dass die im Auftrag zu verarbeitenden Daten nur entsprechend der Auftragsbestätigung verarbeitet werden. Dies beinhaltet strenge Verfahren zur Überprüfung und Kontrolle von Datenzugriffen, genaue Dokumentation von Datenverarbeitungsprozessen, Protokollierung von Aktionen, die mit Datenverarbeitung in Zusammenhang stehen, und regelmäßige Audits. Auftragskontrollmaßnahmen beinhalten zudem auch die Überprüfung von Subunternehmern, um die Einhaltung von Datenschutzbestimmungen sicherzustellen.

6. Verfügbarkeitskontrolle

Diese Maßnahmen umfassen Systemredundanzen, Disaster Recovery-Strategien, fortlaufende Überwachung unserer Systeme und Netzwerke, regelmäßige Aktualisierungen und Patches sowie Schulungen des Personals, um sicherzustellen, dass sie sich der Bedeutung der Aufrechterhaltung der Verfügbarkeit bewusst sind. Dadurch wird die Kontinuität der Geschäftstätigkeit gewährleistet und das Risiko von Datenverlust oder -unterbrechung minimiert.

7. Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken: Die Systeme des Auftragnehmers werden von mehreren Mandanten gleichzeitig genutzt (Mandantenfähigkeit) und gewährleisten eine logische Trennung der Daten der Mandanten. Gleichzeitig besteht eine physikalische Trennung der Systeme nach Funktion in Entwicklungssystem, Testsystem und Produktivsystem.

Anlage 2 – Eingesetzte Subdienstleister

Erbrachte Leistungen	**Anbieter**	**Verarbeitete Daten**
IT-Infrastrukturleistungen (Server)	Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg	Technische Protokolldaten
Email und SMS-dienstleister	Sendgrid, Twilio Germany GmbH, Unter den Linden 10, 10117 Berlin	Technische Protokolldaten, Kontaktdaten
Chat-Funktion	Firebase, Google Ireland Ltd, Gordon House Barrow Street Dublin 4, D04E5W5 Ireland	Technische Protokolldaten Identifikationsdaten
Datenbank	MongoDB Inc., 1633 Broadway 38th Floor New York, NY 10019, USA	Identifikationsdaten Kontaktdaten Geolokationsdaten Weitere personenbez. Daten zB in Freitextfeldern
Fehlermeldungssystem	Functional Software, Inc. dba Sentry, 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Technische Protokolldaten
Fehlermeldungs- und Sicherheitssystem	Cloudflare Inc, 101 Townsend St, San Francisco, California, USA	Technische Protokolldaten Identifikationsdaten
Analytics	Amplitude Inc. 201 3rd Street, Suite 200 San Francisco, CA 94103, USA	Technische Protokolldaten
lets Admin Funktionalitäten	ReTool Inc., 292 Ivy Street, San Francisco, California, USA	Technische Protokolldaten Identifikationsdaten (User-ID)