VERTRAG

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

Mag. Dr. Johannes Pöschl, c/o lets-meet.org, Stöberplatz 4, 1160 Wien,
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Vertrags

(1) Gegenstand

Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Verwaltung von Events, Eventanmeldungen und Kontaktdaten entsprechend der Vorgaben des Auftraggebers

(2) Dauer

(1) Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Nutzung der Dienste des Auftragsverarbeiters.

(2) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(3) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas Anderes.

2. Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer verwaltet die Daten der Events, welche vom Auftraggeber angelegt werden. Diese Daten umfassen u.a. Eventdetails (z.B. Zeit, Ort, E-Mail Adresse des Organisators) und Teilnehmerdaten wie z.B. Name und E-Mail Adresse. Zusätzliche personenbezogene Teilnehmerdaten können vom Auftraggeber bei der Eventanmeldung abgefragt werden, z.B. Telefonnummer oder Firmenname.

Weiters können Kontaktdaten der Kunden des Auftraggebers im System verwaltet werden. Kunden des Auftraggeber erhalten außerdem Benachrichtigungen vom Auftragnehmer, etwa bei erfolgter Eventanmeldung oder falls diese vom Auftraggeber zu einem Event eingeladen werden.

Darüber hinaus können personenbezogene Daten bei der Übermittlung von Feedback und bei der Durchführung von Bestellungen verarbeitet werden.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Firmenstammdaten (Firmenname, Firmenbuchnummer, UID-Nummer)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Eventspezifische, personenbezogene Daten, die vom Auftraggeber bei Eventanmeldung abgefragt werden

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- User des Kunden / Eventteilnehmer
- Beschäftigte des Kunden
- Ansprechpartner des Kunden

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.

4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der

Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu.
Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Die Auslagerung auf Unterauftragnehmer und der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die unter üblichen Umständen 14 Tage nicht unterschreiten darf, im Falle von technischen oder anderweitigen akuten Problemen aber auch nur 24 Stunden betragen darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller

Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO.

Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage werden die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen

und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, technisch mit vertretbarem Aufwand nicht verhinderbare Kopien (z.B. in Log Dateien) sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber drei Monate nach Beendigung einer etwaigen Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Anlage 1 - Technisch-organisatorische Maßnahmen

Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen.

1. **Pseudonymisierung**

Der komplette Nachname der Eventteilnehmer ist nur für den Auftraggeber sichtbar und wird je nach Vorgabe des Auftraggebers für alle anderen Teilnehmer entweder komplett ausgeblendet, oder durch den ersten Buchstaben des Nachnamen ersetzt. Weitere personenbezogene Daten von Eventteilnehmern wie E-Mail Adresse oder Telefonnummer sind nur für den Auftraggeber sichtbar.

2. **Vertraulichkeit**

- Schutz vor unbefugter Systembenutzung durch Passwörter
- Strenge Vorkehrungen um unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems zu verhindern

3. **Integrität - Weitergabekontrolle:**

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung durch 256-bit TLS 1.2 Verschlüsselung aller Übertragungen zwischen Auftraggeber und Auftragnehmer
- Verschlüsselung von Source Code Backups
- Verschlüsselte Übertragung aller Daten zwischen Auftraggeber und Hostingpartner

4. **Integrität – Eingabekontrolle:**

- Protokollierung der erzeugten Daten nach Nutzern
- Protokollierung des letzten Logins jedes Nutzers
- Protokollierung der Uhrzeit der letzten Änderung von Events, Benutzerkonten, Kontakten, Teilnehmerdaten, usw.
- Verhinderung und Protokollierung von unbefugten Lese- oder Schreibzugriffen

5. **Verfügbarkeit und Belastbarkeit**

- Regelmäßige Kontrollen des Systemzustandes (Monitoring)
- Der Auftraggeber sichert laufend den Source Code der Applikationen
- Virenscanner und Firewalls sind auf allen Systemen aktiv, die zur Datenverarbeitung verwendet werden
- Geschäftsrelevante Datenverarbeitungssysteme des Hosting Partners sind redundant vorhanden

- Im Rahmen eines strukturierten Backup-Plans werden Daten in regelmäßigen Abständen vom Hosting Partner gesichert. Dies ermöglicht eine schnelle Wiederherstellung der Daten im Notfall.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Laufende Überprüfung und Weiterentwicklung der Mechanismen, die unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems verhindern
- Unbefugte Zugriffversuche werden geloggt und zwei Mal wöchentlich per E-Mail versandt und laufend evaluiert

7. Zutrittskontrolle: Schutz der Datenverarbeitungsanlagen

- Gesicherter Eingang
- Rigorose Zutrittsbeschränkungen beim Hostingpartner, um physische Sicherheit der Daten zu gewährleisten (Automatische Schließung der Zugangstüren, Kameraüberwachung, Bewegungserkennung, Direkt-Alarmierung der verantwortlichen Mitarbeiter über redundante Kommunikationswege, Workstations mit verschlossenen Metallgehäusen, Datenträger nicht von außen zugänglich, …)

8. Zugangskontrolle

- Identifikation sowie Berechtigungsprüfung eines Benutzers
- Bildschirm- und Computersperre bei Verlassen des Arbeitsplatzes
- Festlegung und Kontrolle der Zugangsbefugnisse

9. Zugriffskontrolle: Schutz vor unbefugter Applikationsnutzung

- Berechtigungs- und Rollenkonzept für Applikationen
- Funktionsbegrenzung (funktionell/zeitlich)
- Trennung von Entwicklungs- und Produktivsystemen
- Schutz der Benutzerkonten mit Passwörtern, die technischer Vorgaben entsprechen müssen
- Automatische Sperrung für eine gewissen Zeit bei mehrfachen Login-Fehlversuchen
- Automatische Sperrung für eine gewissen Zeit bei mehrfachen Versuchen, das Passwort zurückzusetzen oder den Link zur Passwortänderung zu erraten
- Die kompletten Teilnehmerlisten von Events (nicht pseudonymisiert), die nach Anlegung eine Accounts erstellt werden, sind nur nach Eingabe von Benutzername und Passwort einsehbar

10. Löschung der Daten

- Eine Löschung der Daten des Auftraggebers, ausgenommen der Bestelldaten für die Buchhaltung, kann vom Auftraggeber selbst im Profil seines Benutzerkontos durchgeführt werden

Wien, 25.9.2023

_____	_____
Ort, Datum	Ort, Datum
	
_____	_____
Auftraggeber	Mag. Dr. Johannes Pöschl

Anlage 2 - Genehmigte Unterauftragsverhältnisse

Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland*
prohost networks GmbH	Wilhelm-Külz-Str. 69 14532 Stahnsdorf Deutschland	Hostingpartner	
Dr. Anna Dremsek	Weißgasse 45/1 1170 Wien	Textierung, Unterstützung bei Support und Buchhaltung	
Google Ireland Limited	Gordon House, Barrow Street Dublin 4 Ireland	Analyse von Webseitenzugriffen im Rahmen von Google Analytics (GA)	GA wird ohne Cookies und mit IP-Anonymisierung eingesetzt. Zudem ist GA auf Seiten deaktiviert, die Eventteilnehmerdaten oder Kundendaten des Auftragnehmers enthalten sowie auf der Bestellseite.

* An dieser Stelle kommen insbesondere die Standarddatenschutzklauseln der Kommission gem. Art. 46 Abs. 2 lit. c DS-GVO in der Variante „Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter“ (Modul 3) in Betracht.