Auftragsverarbeitungsvertrag (Art. 28 DSGVO) von ONLINERY e.U.

Version: 2025-10-05

1. Gegenstand, Geltung, Zustandekommen (Online-Abschluss)

1.1. Gegenstand: Die Auftragsverarbeiterin verarbeitet personenbezogene Daten im Auftrag des Kunden zur Erbringung der im jeweiligen Leistungsangebot (z. B. „Quick-Start Ads – Essential“) beschriebenen Services gemäß Anlage 1.

1.2. Rahmencharakter: Dieser AVV ist Rahmenvertrag und gilt für sämtliche vom Kunden online gebuchten Leistungen der Auftragsverarbeiterin, sofern dabei eine Verarbeitung personenbezogener Daten im Auftrag erfolgt.

1.3. Zustandekommen/Einbeziehung (Clickwrap): Der AVV wird ohne eigenhändige Unterschrift wirksam. Er wird dem Kunden vor Abgabe der Bestellung in zumutbarer Weise bereitgestellt und durch aktives Anklicken einer Zustimmungs-Checkbox bzw. Betätigung eines entsprechend bezeichneten Bestätigungsbuttons (z. B. „Kostenpflichtig bestellen & AVV akzeptieren“) vertraglich einbezogen und abgeschlossen. Die Auftragsverarbeiterin dokumentiert Einbeziehung und Annahme (Zeitstempel, Version, IP/Session-ID, Inhalt).

1.4. Vorrang: Soweit datenschutzrechtliche Fragen betroffen sind, gehen die Regelungen dieses AVV abweichenden Bestimmungen des Hauptvertrags vor.

2. **Dauer, Weisungen, Zweckbindung**

2.1. Dauer: Geltung ab Online-Abschluss bis zur vollständigen Beendigung der jeweiligen Leistungen und ordnungsgemäßen Datenlöschung/-rückgabe nach Ziff. 12.

2.2. Weisungen: Verarbeitung ausschließlich auf dokumentierte Weisungen des Kunden (Art. 28 Abs. 3 lit. a DSGVO). Mündliche/telefonische Weisungen sind schriftlich oder in Textform (E-Mail/Ticketsystem) zu bestätigen.

2.3. Zweckbindung: Keine Verarbeitung zu eigenen Zwecken der Auftragsverarbeiterin.

3. **Kategorien von Daten/Betroffenen**

Die verarbeiteten Datenkategorien und Betroffenengruppen ergeben sich aus Anlage 1 (u. a. Leads/Interessenten/Kunden des Kunden; Kontakt- und Kommunikationsdaten; Online-Kennungen; Nutzungs-/Event-/Conversion-Daten; optional Rechnungs-/Zahlungsdaten).

4. **Vertraulichkeit, Personal**

4.1. Die bei der Auftragsverarbeiterin tätigen Personen sind auf Vertraulichkeit verpflichtet und unterwiesen (Art. 28 Abs. 3 lit. b; Art. 32 DSGVO).

4.2. Zugriff nach Need-to-know und dokumentiertem Rollen-/Berechtigungskonzept.

5. **Technische und organisatorische Maßnahmen (TOMs)**

5.1. Die Auftragsverarbeiterin unterhält angemessene TOMs gem. Art. 32 DSGVO, Details in Anlage 2.

5.2. Wesentliche Verschlechterungen der TOMs bedürfen vorab der Zustimmung des Kunden; Verbesserungen sind jederzeit zulässig.

6. **Unterstützungspflichten**

6.1. Betroffenenrechte: Angemessene Unterstützung des Kunden bei Anträgen nach Art. 12–23 DSGVO.

6.2. DPIA/Konsultation: Unterstützung nach Art. 35/36 DSGVO, soweit die vom Auftrag umfassten Verarbeitungen betroffen sind.

6.3. Nachweise: Bereitstellung erforderlicher Informationen zur Erfüllung der Pflichten aus Art. 28 Abs. 3 lit. h DSGVO.

7. **Verletzung des Schutzes personenbezogener Daten**

7.1. Meldung: Die Auftragsverarbeiterin informiert den Kunden unverzüglich und ohne schuldhaftes Zögern, i. d. R. innerhalb von 24 Stunden nach Kenntniserlangung, über Datenschutzvorfälle (Art. 33/34 DSGVO) und liefert verfügbare Mindestangaben; Nachlieferungen folgen fortlaufend.

7.2. Eindämmung/Behebung: Koordinierte Maßnahmen zur Risikominimierung; Dokumentation des Vorfalls.

8. **Unterauftragsverarbeiter (Sub-Prozessoren)**

8.1. Allgemeine Genehmigung/Liste: Der Einsatz von Unterauftragsverarbeitern ist mit allgemeiner Genehmigung zulässig. Die jeweils aktuelle Liste samt Garantien (SCC/DPF etc.) ist in Anlage 3 dokumentiert und wird bei Änderungen aktualisiert.

8.2. Änderungsmitteilung/Widerspruch: Geplante Änderungen werden dem Kunden mit angemessener Frist mitgeteilt; ein Widerspruch aus wichtigem Datenschutzgrund ist binnen 10 Arbeitstagen möglich.

8.3. Bindung/Haftung: Sub-Prozessoren werden schriftlich mindestens zu den Pflichten dieses AVV verpflichtet (Art. 28 Abs. 4 DSGVO). Die Auftragsverarbeiterin bleibt intern verantwortlich für deren DSGVO-konforme Leistungserbringung.

9. **Internationale Datenübermittlungen**

9.1. Drittlandübermittlungen erfolgen nur bei Vorliegen geeigneter Garantien (z.B. Angemessenheitsbeschluss/DPF, Standardvertragsklauseln inkl. Transfer Impact Assessment und ggf. ergänzender Maßnahmen).

9.2. Die konkret genutzten Mechanismen sind in Anlage 3 ausgewiesen.

10. **Kontrollen, Audits, Auskünfte**

10.1. Auditrecht: Nach angemessener Ankündigung (i. d. R. 14 Tage) kann der Kunde Audits/Inspektionen durchführen oder durch unabhängige Prüfer durchführen lassen, unter Wahrung von Vertraulichkeit, Betriebsabläufen und Rechten Dritter.

10.2. Surrogat-Nachweise: Geeignete Zertifizierungen/Prüfberichte (z. B. ISO 27001, SOC 2) können Audits ergänzen/ersetzen, soweit ausreichend.

11. **Behördenkontakte, Mitwirkung**
    Bei behördlichen Anfragen informiert die Auftragsverarbeiterin den Kunden, soweit rechtlich zulässig, und kooperiert.

12. **Rückgabe und Löschung**

12.1. Nach Vertragsende oder auf Weisung: Rückgabe in gängigem Format und/oder Löschung sämtlicher personenbezogener Daten inkl. Kopien; gesetzliche Aufbewahrung bleibt unberührt.

12.2. Durchführung wird schriftlich bestätigt.

13. **Haftung und Freistellung**
    Parteien haften nach DSGVO und anwendbarem Recht. Die Auftragsverarbeiterin stellt den Kunden von Schäden frei, die aus schuldhafter Verletzung dieses AVV oder datenschutzrechtlicher Pflichten durch sie/ihre Sub-Prozessoren resultieren.

14. **Änderungen, Rang, Textform**

14.1. Änderungen/Ergänzungen dieses AVV erfolgen in Textform, inkl. elektronischer Form (E-Mail/Portal-Update) mit Versionshinweis.

14.2. Bei Widersprüchen zwischen AVV und sonstigen Vereinbarungen hat der AVV Vorrang, soweit Datenschutz betroffen ist.

15. **Recht, Gerichtsstand**

15.1. Österreichisches Recht (ohne Kollisionsnormen).

15.2. Gerichtsstand: Braunau am Inn.

(Kein Unterschriftenfeld erforderlich; Online-Akzeptanz gem. Ziff. 1.3.)

Anlage 1 – Beschreibung der Verarbeitung

- Leistungen/Zwecke: Lead-Erfassung (Wix/HubSpot), Synchronisation/Automationen (Make/HubSpot), Kampagnen-Setup & -Optimierung (Google/Meta/LinkedIn/TikTok), Tracking/Attribution (GA4/GTM), Reporting (Looker Studio), Support.
- Datenkategorien: Stamm-/Kontaktdaten (Name, E-Mail, Telefon), Kommunikationsdaten, Online-Kennungen (Cookies/IDs), Nutzungs-/Event-/Conversion-Daten; optional Rechnungs-/Zahlungsdaten (falls betroffen).
- Betroffene: Website-Nutzer, Interessenten, Kunden des Kunden, B2B-Kontaktpersonen.
- Verarbeitungen: Erheben, Speichern, Organisieren, Übermitteln, Auswerten, Löschen.
- Speicherorte: EU/EWR; ggf. Drittland gem. Anlage 3.
- Speicherdauer/Löschung: Leads z. B. 24 Monate (anpassbar), Kunden: Vertragslaufzeit + 6 Monate; Backups rotierend; individuelle Löschfristen auf Weisung.

- Empfänger: Genehmigte Sub-Prozessoren nach Anlage 3; keine Weitergabe zu eigenen Zwecken.
- Zugriffsmodell: Kunden-Admin verbleibt beim Kunden; Agenturzugänge mit Least-Privilege.

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)

- Organisation: Vertraulichkeitsverpflichtung, jährliche Schulungen, Rollen-/Berechtigungskonzept, Vier-Augen-Prinzip bei kritischen Änderungen, On/Off-Boarding-Prozess.
- Zutritt/Zugriff: MFA, starke Passwörter, Geräteverschlüsselung, Bildschirmsperre, physischer Zugangsschutz.
- Übertragung/Speicherung: TLS 1.2+, Verschlüsselung ruhender Daten, Mandantentrennung, Protokollierung adminrelevanter Ereignisse.
- Trennung/Pseudonymisierung: Projekt-/Kunden-Trennung; Pseudonymisierung/Maskierung wo möglich.
- Backup/BCM: Regelmäßige Backups (anbieterspezifisch), Restore-Tests, Incident-/BCM-Prozess (Anlage 4).
- Lieferantenmanagement: Vorab-Prüfung, DPA/Vereinbarungen, SCC/DPF-Status, regelmäßiges Re-Assessment.
- Löschkonzept: Automatisierte Routinen, Löschprotokolle, Notfall-Löschungen auf Weisung.

Anlage 3 – Genehmigte Unterauftragsverarbeiter (Baseline; kundenspezifisch bestätigend)

- Wix.com Ltd. (IL/EU) – Website/Forms/Payments (falls genutzt) – EU/IL/ggf. weitere – Angemessenheit IL / SCC / ggf. DPF je Dienst
- HubSpot Ireland Ltd. (IE) – CRM/Marketing-Automation/E-Mail – EU/ggf. USA – DPF (falls zert.) / SCC + TIA
- Make a.s. (CZ) – iPaaS/Automationen – EU – SCC für Drittlands-Unterdienste
- Google Ireland Ltd. (IE) – Ads/GA4/GTM/Looker Studio – EU/ggf. global – DPF (falls zert.) / SCC + Zusatzmaßnahmen
- Meta Platforms Ireland Ltd. (IE) – Ads/Business-Tools – EU/ggf. USA – DPF (falls zert.) / SCC
- LinkedIn Ireland Unlimited (IE) – Ads/Insights – EU/ggf. USA – DPF (falls zert.) / SCC
- TikTok Technology Ltd. (IE) – Ads/Pixel/Events – EU/ggf. UK/USA – SCC/UK-IDTA; EU-Rechenzentren je Policy

Anlage 4 – Incident-Runbook (Kurz)

- Erkennen: Monitoring, definierter Meldeweg an datenschutz@onlinery.at.
- Erstmeldung: Binnen 24 h mit Mindestinhalten (Art, Umfang, Kategorien, Folgen, Abhilfen).
- Eindämmung/Behebung: Zugriffssperren, Passwort-Resets, Forensik, Fix-Deployment.
- Dokumentation: Incident-Report, Lessons Learned, TOM-Anpassung.
- Kommunikation: Koordination mit Kunde betreffend Behörde/Betroffene (Art. 33/34).