Austria Design · Schießgraben 5/28 · 2500 Baden

.....
.....
.....
.....

Vereinbarungserklärung

Gegenstand:
Auftragsverarbeitung nach Art. 28 DSGVO (Domain & E-Mail)
Version 1.2

Zwischen	.....	und	**Austria Design / Agency for Creativity**
	.....		**Herr Stefan Biba**
Verantwortlicher:	.....	Auftragsverarbeiter:	**Schießgraben 5/28**
(Auftraggeber)	.....	(Auftragnehmer)	**2500 Baden**
	.....		**Österreich**

AUSTRIA-DESIGN.AT

1. Gegenstand der Vereinbarung

(1) Gegenstand dieser Vereinbarung ist die Durchführung folgender Aufgaben: Registrierung/Transfer/Konfiguration einer oder mehrerer TLD-Domains bei unserem Partnerprovider zur Erreichbarkeit von Web- und E-Mail-Services, Erstellung und initiale Konfiguration eines Webspeicherplatzes auf einem unserer gehosteten Virtual Server zum Speichern von Website-Inhalten/Datenbanken/Applikationen/E-Mails, Setzung von sicheren Initialpasswörtern als Zugriffsschutz vor unbefugten Dritten, Erstellung von kostenlosen X.509-SSL-Zertifikaten bei der Zertifizierungsstelle letsencrypt.org (EFF, Mozilla, U-M) inkl. automatischer kostenloser Zertifikatsverlängerung für alle TLD-Domains zur sicheren Übertragung von Daten über Website- und E-Mail-Gateway, automatische und kostenfreie Aktualisierungen von Server-Betriebssystem-Updates, Wordpress-Hauptversionen und Plugins zum Schutz vor schwerwiegenden Programmfehlern, automatische Erstellung und Konfiguration einer „GA-Tracking-Property" (Cookie) zum Sammeln analytischer, anonymisierter Daten via Google Analytics, Erstellung eines kostenlosen Eintrags auf Google My Business zur Auffindbarkeit des Unternehmens bei Google Maps, Erstellung eines kostenlosen Eintrags auf Google Search Console zur Suchmaschinenoptimierung Standard, Erstellung eines automatischen, verschlüsselten und benutzerspezifischen Backups auf einem unserer Virtual-Server und in Google Drive mit allen zum Webspeicherplatz zugehörigen Dateien (Website-Inhalte, Datenbanken, Applikationen (Wordpess usw.) inkl. Plugins, E-Mails, Konfigurationen/Einstellungen, verschlüsselte Passwörter) jeden Montag um 03:00 Uhr (MEZ) zur Wiederherstellung von fehlerhaften/versehentlich gelöschten Dateien und Konfigurationen, technische Hilfeleistung und Remote-Einrichtung für Fehlerbehebungen über das verschlüsselte Ticketsystem help.austria-design.at in Kooperation mit dem technischen Server-Supportteam des IT-Rechenzentrums in Deutschland, optionale kundenspezifische (kostenpflichtige) Aufträge wie das Einrichten von Newsletter-Systemen inklusive Erstellung von Benutzerkonten, Newsletter-Kampagnen und Versand an Abonnenten, technische Erweiterungen oder Entfernen von Teilkomponenten verschiedener Web-Applikationen (Websites, Applikationen etc.), Beauftragung Dritter zur Vertragserfüllung, sichere Rechnungslegung über einen Cloud-Dienstleister für eine steuerkonforme und gesetzliche Abwicklung von Zahlungen unserer Leistungen und Produkte inklusive Zahlungsabgleich mit unserem Bankkonto und automatisiertem Erinnerungs- und Mahnsystem.

(2) Folgende Datenkategorien werden verarbeitet: Personenstammdaten (Firmenname, Vor- und Nachname, Adresse, E-Mail-Adresse, Telefonnummer), Kommunikationsdaten (z. B. Telefon, E-Mail), Vertragsabrechnungs- und Zahlungsdaten (IBAN, BIC und Bankinstitut, Zahlungshistorie, Mahnstufen).

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte

2. Dauer der Vereinbarung

Die Vereinbarung gilt auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 7 Werktagen vor Vertragsverlängerung gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

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 eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(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 nach Art. 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO 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 wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten . Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Ort der Durchführung der Datenverarbeitung

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

5. Unterauftragsverhältnisse

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

(2) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftragsverarbeitungsvertrag dem Unterauftragnehmer zu übertragen.

(3) Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls 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. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. Salvatorische Klausel, Gerichtsstand

(1) Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

(2) Als Gerichtsstand wird Baden vereinbart.

Ort, Datum

Unterschrift Auftraggeber

Baden, am

Ort, Datum

Unterschrift Auftragnehmer

AUSTRIA-DESIGN.AT

Anlage:

Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO

Bitte senden Sie das vollständig ausgefüllte und unterzeichnete Formular per E-Mail an hello@austria-design.at oder per Post an Austria Design, Schießgraben 5/28, 2500 Baden

Anlage 1 – Technisch-organisatorische Maßnahmen

Vertraulichkeit

(1) Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, elektrische Türöffner;

(2) Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

(3) Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis", Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten;

(4) Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

(5) Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

(1) Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung;

(2) Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Verfügbarkeit und Belastbarkeit

(1) Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;

(2) Rasche Wiederherstellbarkeit;

(3) Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(1) Datenschutz-Management;

(2) Incident-Response-Management;

(3) Datenschutzfreundliche Voreinstellungen;

(4) Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.