

Auftragsdatenbearbeitungsvereinbarung

1. Gegenstand der Vereinbarung

- a. webagentur.ch AG ("webagentur.ch") erbringt gegenüber dem Kunden Webseiten-Dienstleistungen. Bei der Erbringung der Dienstleistungen speichert webagentur.ch personenbezogene Daten im Auftrag und für die Zwecke des Auftraggebers. Diese Vereinbarung zur Auftragsdatenverarbeitung regelt die Pflichten, Rollen und Zuständigkeiten von webagentur.ch und dem Auftraggeber ("Kunde") in Bezug auf die Auftragsverarbeitung.
- b. Die Bestimmungen dieser ADV-Vereinbarung schränken die Rechte und Pflichten der Vertragsparteien in Bezug auf die Erbringung bzw. die Inanspruchnahme der Webseiten-Dienstleistungen nicht ein.

2. Pflichten von webagentur.ch

- a. webagentur.ch verpflichtet sich, die personenbezogenen Daten nur zur Erbringung der Webseiten-Dienstleistungen im Rahmen des Servicevertrags und vertraglichen Pflichten sowie gemäss dieser ADV-Vereinbarung zu verarbeiten.
- b. webagentur.ch verpflichtet sich, alle erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die Sicherheit der Daten zu gewährleisten.
- c. webagentur.ch verpflichtet sich, Mitarbeiter mit Zugang zu den personenbezogenen Daten zur Wahrung der Vertraulichkeit (auch über die Dauer ihrer Tätigkeit für webagentur.ch hinaus) zu verpflichten.
- d. webagentur.ch informiert den Kunden unverzüglich, wenn sie der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften. webagentur.ch ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.
- e. webagentur.ch verpflichtet sich, den Kunden ohne Verzug schriftlich zu informieren, wenn webagentur.ch Kenntnis von einer Datensicherheits-Verletzung erlangt, die personenbezogene Kunden-Daten betrifft. Dabei hat webagentur.ch dem Kunden die Art und das Ausmass der Verletzung sowie mögliche Abhilfemassnahmen mitzuteilen.
- f. Die Löschung der personenbezogenen Kunden-Daten nach Ende der Laufdauer des Hosting-Vertrags richtet sich nach den gesetzlichen Vorgaben

3. Pflichten des Kunden

- a. Der Kunde trifft in seinem Verantwortungsbereich selbstständig angemessene technische und organisatorische Massnahmen zum Schutz der personenbezogenen Daten.
- b. Der Kunde ist für die Rechtmässigkeit der Verarbeitung der personenbezogenen Daten, einschliesslich der Zulässigkeit der Auftrags- bzw. Unter-Auftragsverarbeitung, verantwortlich.

4. Subunternehmer

- a. Beansprucht der Kunde Dienstleistungen von webagentur.ch, die personenbezogene Daten betreffen und durch Subunternehmer erbracht werden, bleibt webagentur.ch, gegenüber dem Kunden Auftragsverarbeiterin und erfüllt die diesbezüglichen Pflichten aus der ADV-Vereinbarung.
- b. Webagentur.ch darf zur Erfüllung seiner Verpflichtungen gemäß diesem Vertrag Subunternehmer einsetzen. webagentur.ch ist jedoch verpflichtet, den Kunden über den Einsatz von Subunternehmern zu informieren und sicherzustellen, dass diese die gleichen Datenschutzstandards einhalten.
- c. Die Zustimmung gilt generell als erteilt für alle Subunternehmer, die zum Zeitpunkt des Vertragsschlusses in der Liste in «Anhang 3» aufgeführt werden.

5. Kontrollrechte

- a. Der Kunde hat das Recht, die Einhaltung der datenschutzrechtlichen Bestimmungen durch webagentur.ch zu überprüfen. Webagentur.ch verpflichtet sich, dem Kunden alle erforderlichen Informationen und Unterlagen zur Verfügung zu stellen, um eine solche Überprüfung zu ermöglichen.
- b. Die vorstehenden Kontrollrechte des Kunden bestehen unter dem Vorbehalt des Verhältnismässigkeitsgebots und der Wahrung der schutzwürdigen Interessen (insbesondere Sicherheits- oder Geheimhaltungsinteressen) von webagentur.ch. Besteht keine anderslautende Vereinbarung zwischen den Vertragsparteien trägt der Kunde sämtliche Kosten der Information und Prüfung, einschliesslich nachgewiesener interner Kosten von webagentur.ch.

Anhang 1: Beschreibung der Datenbearbeitung

1. Kategorien möglich betroffener Personen, deren Personendaten bearbeitet werden:

- Webseiten-Besucher wie Kunden, Interessenten, Fans, ...
- Mitarbeitende, freie Mitarbeitende (aktuell und ehemalig), Bewerber
- Lieferanten und Geschäftspartner, externe Partner

2. Kategorien der möglichen bearbeiteten Personendaten

- Kundendaten (z.B. Geschlecht, Anschrift, Namen, Telefonnummer, E-Mail-Adresse)
- Mitarbeiterdaten (z.B. Geschlecht, Namen, Telefonnummer, E-Mail-Adresse)
- Kontaktinformationen (z.B. Firma, E-Mail, Telefon, physische Geschäftsadresse)
- Vertragsstamm- und Finanzdaten (z.B. Vertragsbeziehung, Produkt- bzw. Abrechnungsdaten)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Termin-, Planungs- und Steuerungsdaten

3. Zwecke der Bearbeitung

- Vertragserfüllung resp. Bereitstellung der Webseite
- Kontaktaufnahmen über Anfrage-Formulare von Webseiten
- Bestellungen über Webshops von Webseiten

Anhang 2: Beschreibung der ergriffenen technischen und organisatorischen Massnahmen von webagentur.ch

Zutrittskontrolle

Massnahmen, mit denen Unbefugten der Zutritt zu Datenbearbeitungsanlagen verwehrt wird, mit denen Personendaten bearbeitet oder genutzt werden:

- Schlüssel-Management (Schlüssel-Herausgabe, etc.)
- Besucherregistrierung und Besuchermanagement
- Sicherheitsschlösser
- Sorgfältige Auswahl des Reinigungspersonals

Zugangskontrolle

Massnahmen, mit denen die Nutzung von Datenbearbeitungssystemen durch Unbefugte verhindert wird:

- Vergabe von Benutzerrechten
- Passwortvergabe
- Authentifizierung mit Benutzername / Passwort
- Minimalvoraussetzungen für Passwortkomplexität
- Verwendung von Virenscannern
- Verwendung einer Software Firewall

Zugriffskontrolle

Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenbearbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass Personendaten bei der Bearbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

- Schaffung eines Autorisierungskonzepts (Identity Access Management),
- Anzahl Administratoren aufs "absolute Minimum" reduziert
- Sichere Medienbereinigung vor der Wiederverwendung
- Rechteverwaltung durch Systemadministratoren
- Passwort-Richtlinie mit Vorgaben zur Passwortlänge
- Sichere Aufbewahrung von Datenträgern

Bekanntgabe Kontrolle

Massnahmen, die gewährleisten, dass Personendaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Personendaten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Dokumentation der Datenempfänger
- Hardware-Verschlüsselung
- TLS-Verschlüsselung für Mail Kommunikation

Eingabekontrolle

Massnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem Personendaten in Datenbearbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Protokollierung der Eingabe, Modifikation und Löschung von Daten,
- Rückverfolgbarkeit der Eingabe, Modifikation und Löschung von Daten durch individuelle User
- Rechtevergabe für Eingabe, Modifikation und Löschung von Daten basierend auf einem Autorisierungskonzept

Verfügbarkeitskontrolle

Massnahmen, die gewährleisten, dass Personendaten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Erstellen von Datenbackups
- Testen der Datenwiederherstellung
- Sichere off-site Speicher von Datenbackups

Gebot der Trennung

Massnahmen, die gewährleisten, dass Personendaten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt bearbeitet werden:

- Schaffung eines Autorisierungskonzepts
- Bewilligte und dokumentierte Datenbankrechte
- Trennung von produktiven und Testsystemen

Anhang 3: Subauftragsbearbeiter von webagentur.ch

Unternehmen	Zweck	Ort / Land
Kreativ Media GmbH	Hosting / Server	Zürich / Schweiz
Bando Treuhand AG	Treuhand, Revision	Basel / Schweiz
Fiducial Winbiz SA	Buchhaltungssoftware	Genf / Schweiz