

(AVV)

Vereinbarung zur Auftragsverarbeitung

Nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Dieser Vertrag muss nicht (kann aber auf Wunsch in Schriftform übersendet werden) unterschrieben werden, da er fester Bestandteil der AGB des Tätigwerdens des Auftragsverarbeiters ist. Der Verantwortliche / Kunden kann diesem Vertrag jederzeit widersprechen.

In diesem Fall werden online gestellte Daten kurzfristig bis zur Klärung des Sachverhalts offline gestellt.
Der Auftragsbearbeiter ist nicht verpflichtet, dem Verantwortlichen / Kunden hieraufhin speziell hinzuweisen.

zwischen

[Name des Verantwortlichen / Kunden]

Adresse: [Adresse]

Telefon: [Telefonnummer]

E-Mail: [E-Mail-Adresse]

(im Folgenden „Verantwortlicher“ oder „Kunde“ genannt)

und

des Auftragsverarbeiters

uxcommerce / uxsoft

vertreten durch Manfred Bichof

Manfred Bischof

POB 143 (ladungsfähige Anschrift)

20 300 Loutraki Greece

im folgenden Auftragsverarbeiter genannt.

Präambel

Dieser Auftragsverarbeitungsvertrag regelt die Bedingungen, unter denen der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen / Kunden verarbeitet. Dieser Vertrag basiert auf den Anforderungen der Datenschutz-Grundverordnung (DSGVO), insbesondere Art. 28 DSGVO.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand der Verarbeitung:

Der Auftragsverarbeiter stellt dem Verantwortlichen Hosting-Dienstleistungen zur Verfügung, insbesondere:

- Betrieb und Wartung von Servern

- Speicherung und Verwaltung von personenbezogenen Daten
- Durchführung von Backups
- Monitoring und Wartung der IT-Infrastruktur

Dauer der Verarbeitung:

Die Verarbeitung beginnt mit der Unterzeichnung dieses Vertrags und endet mit der Beendigung der Geschäftsbeziehung oder auf Wunsch des Verantwortlichen.

In der Regel ergibt sich der Vertrag auch aus der Zustellung von Leistungsrechnungen und der in den Rechnungen bezeichneten Leistungen. In der Rechnung ist in der Regel ein genauer Zeitpunkt der Leistungserbringung angegeben.

Der Vertrag endet sofort, wenn der Auftraggeber (Kunde) mit Rechnungen in Verzug ist. In diesem Zusammenhang wird darauf hingewiesen, dass der Verzug nach Rechnungsstellung und deren erfolgreicher Zustellung (auch auf dem elektronischem Weg) eintritt.

Um diesem Verzug zu entgehen, hat der Kunde die Möglichkeit, Rechnungen z.B. per Sofortüberweisung oder Paypal zu begleichen.

Hintergrund ist, dass nicht der Kunde erwägt, wann oder ob er überhaupt irgendwann Leistungen bestellt und bezahlt. (You get what you paid – Kunde bekommt, was er zahlt)

In keinem Fall haftet der Auftragnehmer für Leistungen, die nicht vom Kunden beim Eintritt eines Schadens bezahlt worden sind.

§ 2 Art und Zweck der Verarbeitung

Art der Verarbeitung:

Erhebung, Speicherung, Nutzung, Organisation, Löschung und ggf. Anonymisierung personenbezogener Daten.

Zweck der Verarbeitung:

Bereitstellung und Wartung von Hosting-Diensten zur Sicherstellung der Erreichbarkeit und Verfügbarkeit der Website bzw. Anwendung des Verantwortlichen.

§ 3 Art der verarbeiteten Daten und betroffene Personen

Art der verarbeiteten Daten:

- Namen
- Adressen
- E-Mail-Adressen
- Telefonnummern
- IP-Adressen
- Nutzungsdaten
- Kommunikationsinhalte

Kategorien betroffener Personen:

- Kunden

- Nutzer
 - Mitarbeiter
-

§ 4 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich, in Bezug auf die Verarbeitung der Daten:

1. **Nur auf dokumentierte Weisung** des Verantwortlichen zu handeln, es sei denn, es ist gesetzlich etwas anderes erforderlich.
2. **Vertraulichkeit** der personenbezogenen Daten zu wahren und sicherzustellen, dass alle mit der Verarbeitung beschäftigten Personen zur Vertraulichkeit verpflichtet sind.
3. **Technische und organisatorische Maßnahmen** gemäß Art. 32 DSGVO zu treffen, um die Sicherheit der Verarbeitung zu gewährleisten.
4. **Unterauftragsverarbeiter nur mit vorheriger Zustimmung** des Verantwortlichen einzusetzen und sicherzustellen, dass diese ebenfalls den Anforderungen der DSGVO entsprechen.

Diese Pflicht zur Zustimmung entfällt, wenn der Unterauftragsverarbeiter z.B. für die Durchführung von Kundenwünschen erforderlich ist. Hierzu fallen in allen Fällen die Registrierungsstellen von Domains.

§ 5 Pflichten des Verantwortlichen

Der Verantwortliche ist verpflichtet, sicherzustellen, dass:

1. **Die Rechtsgrundlage für die Verarbeitung** der personenbezogenen Daten vorliegt.
 2. **Betroffenenrechte** wie Auskunft, Berichtigung, Löschung oder Widerspruch gemäß DSGVO gewahrt werden.
 3. **Die Aufklärung der betroffenen Personen** über die Datenverarbeitung erfolgt (z. B. Durch die auf der Webseite von uxcommerce / uxsoft veröffentlichte Datenschutzerklärung).
 4. **Sicherheitsvorkehrungen und Verfahren** zur Sicherstellung der ordnungsgemäßen Datenverarbeitung getroffen werden.
-

§ 6 Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter darf Unterauftragsverarbeiter nur nach vorheriger Zustimmung des Verantwortlichen einsetzen. Die Zustimmung gilt spätestens als erteilt, wenn die dazugehörige Kostenrechnung beglichen wurde

(2) Der Auftragsverarbeiter hat sicherzustellen, dass für alle Unterauftragsverhältnisse die gleichen Datenschutzpflichten wie in diesem Vertrag geregelt sind.

Liste der Unterauftragsverarbeiter (falls bereits bekannt):

- in der Regel nutzen wir für die gewerblichen Server das
Vautron Rechenzentrum AG
Obermünsterstr. 9
93047 Regensburg

- für die Domainregistrierung von .de-Domains

DENIC eG
Theodor-Stern-Kai 1
60596 Frankfurt am Main

- weitere Registrierungsstellen, zu denen persönliche Daten wie z.B. Domaininhaber übermittelt werden.
- Diverse Mailanbieter, welche dem Auftraggeber bekanntgegeben werden, falls diese in Anspruch genommen werden.

HINWEIS: Kein Unterauftragsverarbeiter liegt im Sinne dieses Vertrages vor, wenn der Kunde / Auftragnehmer Drittanbietersoftware z.B. auf seiner Webseite nutzt.

§ 7 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten getroffen. Eine detaillierte Übersicht der Maßnahmen wird in **Anlage 1** dieses Vertrages aufgeführt.

§ 8 Kontrolle und Nachweise

Der Verantwortliche hat das Recht, die Einhaltung dieses Vertrages und der Datenschutzbestimmungen zu überprüfen. Der Auftragsverarbeiter stellt dem Verantwortlichen alle notwendigen Nachweise zur Verfügung, um die Einhaltung der vereinbarten Maßnahmen zu belegen.

Diese Kontrollmöglichkeit entfällt, wenn der verantwortliche Kunde durch eigene und einfache Recherche dazu in der Lage ist, die Vertragsinhalte selbst zu überprüfen.

Das ist auf jedem Fall möglich, seine eigene IP der Webauftitte zu recherchieren und auch Auskünfte bei den Domainvergabestellen zu erhalten.

§ 9 Datenschutzverletzungen

Im Falle einer Datenschutzverletzung informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, jedoch spätestens innerhalb von 24 Stunden, nachdem er davon Kenntnis erlangt hat.

§ 10 Vertragsbeendigung und Rückgabe von Daten

Nach Beendigung des Vertrages hat der Auftragsverarbeiter alle personenbezogenen Daten, die im Rahmen der Verarbeitung erhoben wurden, entweder an den Verantwortlichen zurückzugeben oder gemäß den Weisungen des Verantwortlichen zu löschen.

§ 11 Sonstiges

1. **Änderungen und Ergänzungen** dieses Vertrages bedürfen der Schriftform.
2. **Gerichtsstand** ist der Sitz des Verantwortlichen, soweit gesetzlich zulässig.
3. Sollte eine Bestimmung dieses Vertrages unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

1. Physische Sicherheitsmaßnahmen

Zugangskontrolle:

- **Zutrittskontrollen:** Nur autorisierte Mitarbeiter haben Zugang zu den beauftragten Rechenzentren. Diese sind in der Regel TÜV zertifiziert. Dies erfolgt oft über **biometrische Systeme** (z. B. Fingerabdruck, Iris-Scan) oder **Schlüsselkarte**.
- **24/7 Überwachung:** Kameras und Sicherheitskräfte überwachen das Gelände rund um die Uhr, um unbefugten Zutritt zu verhindern.

Brand- und Feuerschutz:

- **Brandschutzsysteme:** Rechenzentren sind mit **Sprinkleranlagen** und **Feuerlöschsystemen** ausgestattet, die eine Brandgefahr minimieren.
- **Feueralarmsysteme:** Automatische Detektoren für Rauch und Hitze sowie Alarmsysteme, die eine sofortige Evakuierung auslösen können.

Physische Infrastruktur:

- **Redundante Stromversorgung:** Bei Ausfällen wird auf **Notstromaggregate** und **USV-Systeme (Unterbrechungsfreie Stromversorgung)** zurückgegriffen, um den Betrieb ohne Unterbrechung aufrechtzuerhalten.
-

2. Technische Sicherheitsmaßnahmen

Datenverschlüsselung:

- **Verschlüsselung im Ruhezustand und während der Übertragung:** Daten werden sowohl während der Speicherung als auch bei der Übertragung zwischen Systemen verschlüsselt (z. B. AES-256, TLS/SSL).
- **Ende-zu-Ende-Verschlüsselung** schützt die Daten auch vor Abhörversuchen, besonders bei sensiblen Informationen.

Firewall- und Netzwerkschutz:

- **Firewalls** und **Intrusion Detection Systems (IDS)** schützen vor Angriffen von außen und erkennen **unbefugte Zugriffsversuche**.

- **VPNs (Virtual Private Networks)** werden verwendet, um den Datenverkehr innerhalb des Rechenzentrums zu sichern.
- Jeder Kunde ist zudem in der Lage, kostengünstige VPNs für eigene Zwecke zu buchen.

Redundanz und Ausfallsicherheit:

- **Redundante Systeme:** Server, Netzwerkverbindungen und Stromversorgungen sind mehrfach redundant ausgelegt, sodass beim Ausfall eines Teilsystems der Betrieb weiterhin gewährleistet bleibt.
- Der Auftragsverarbeiter achtet auf die Auslastung der Server. Überbuchte Server werden nicht genutzt.

Backup-Systeme:

- **Datensicherung und -wiederherstellung:** Rechenzentren führen regelmäßige **Backups** durch und haben Verfahren zur **Datenwiederherstellung** im Falle eines Ausfalls.
- Der Kunde erhält mit Auslieferung seiner Webseite (in der Regel) ein integriertes Backupsystem, welches leicht zu bedienen ist, bzw. kostenpflichtig automatisiert läuft.
- Uxsoft stellt als kostengünstige Alternative backups und updates zur Verfügung, die jeder Kunde im Rahmen eines Wartungsvertrages wahrnehmen kann.

Sollte der Kunde selbständig seine Webseite mit Inhalten und Updates versorgen, stellt er den Auftragnehmer von jeglicher Gewähr bezüglich verlorener und untergegangenen Daten und Inhalten frei.

- Sollte eine Webseite aufgrund Eingriffen seitens des Auftraggebers untergehen oder nicht mehr verfügbar sein, wird bei einem bestehenden Wartungsvertrag mit Auftragnehmer und Auftragnehmer versucht, diese schnellstmöglich wieder herzustellen.
- Auch ohne Wartungsvertrag kann der Auftraggeber den Auftragnehmer mit der Wiederherstellung der Daten und dem Beziffern einer möglichen Datenpanne beauftragen. Hierzu werden Kosten-jeweils nach Schätzung- vorab fällig. (<https://uxsoft.de/preisliste> Kosten siehe Support Webseite)

Überwachungssysteme:

- **Monitoring:** Permanente Überwachung der Server- und Netzwerkinfrastruktur hilft dabei, **Fehler** oder **Angriffe** frühzeitig zu erkennen und zu beheben.
- **Protokollierung:** Sicherheitsrelevante Ereignisse und Zugriffe werden in **Log-Dateien** protokolliert, um bei Verdacht auf unbefugte Zugriffe forensische Untersuchungen durchzuführen.

3. Organisatorische Sicherheitsmaßnahmen

Zugriffs- und Berechtigungsmanagement:

- **Role-Based Access Control (RBAC):** Mitarbeiter erhalten nur den **Zugang** zu den Systemen und Daten, die sie für ihre Arbeit benötigen.
- **Mehr-Faktor-Authentifizierung (MFA):** Zur Verstärkung der Authentifizierung werden mehrere Sicherheitsfaktoren kombiniert, wie Passwörter und Einmalcodes.

Mitarbeiterschulungen:

- **Sicherheitsschulungen** für Mitarbeiter, um **Phishing-Angriffe** und andere Bedrohungen zu

erkennen und darauf richtig zu reagieren.

- **Vertraulichkeitsvereinbarungen** und strenge **Personalüberprüfungen** beim Eintritt ins Unternehmen.

Notfallpläne:

- **Business Continuity Plans (BCP)** und **Disaster Recovery Plans (DRP)**: Rechenzentren haben detaillierte Notfallpläne, die festlegen, wie auf **Störungen** oder **Desaster** reagiert wird, um die Datenintegrität zu sichern und den Betrieb wiederherzustellen.
- **Regelmäßige Tests** der Notfallmaßnahmen (z. B. Fire-Drills, Blackout-Simulationen).

Compliance und Zertifizierungen:

- Rechenzentren müssen häufig verschiedene **Compliance-Anforderungen** erfüllen, wie z. B. **ISO 27001** (Informationssicherheitsmanagement), **SOC 2** (Security, Availability, Processing Integrity, Confidentiality, Privacy) oder **PCI-DSS** (für die Verarbeitung von Kreditkartendaten). Kunden haben die Möglichkeit, die Rechenzentren und deren Zertifizierungen aktuell auf deren webseite einzusehen.
 - **GDPR-konform**: Insbesondere europäische Rechenzentren müssen die Anforderungen der **DSGVO** (Datenschutz-Grundverordnung) erfüllen.
-

4. Sicherheitsstandards und Zertifizierungen

- **ISO 27001**: Standard für das Management von Informationssicherheit.
-

5. Datenschutzmaßnahmen

- **DSGVO-konform**: Rechenzentren in Europa müssen sicherstellen, dass sie den **Datenschutzanforderungen** der **DSGVO** entsprechen, insbesondere bei der Speicherung und Verarbeitung personenbezogener Daten.
- **Datenresidenz**: In vielen Fällen müssen Rechenzentren sicherstellen, dass Daten innerhalb bestimmter geografischer Grenzen gespeichert werden, um die lokalen Datenschutzvorschriften zu erfüllen.