Tel.: +49 8654 4042002 support@alldomains.hosting
FAX: +43 6215 20889 www.alldomains.hosting

Anhang 2 zum Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

1. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b DSGVO

- **Zutrittskontrolle**
  Der Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen ist gewährleistet durch:
  - Portier, Sicherheitspersonal und Sicherheitsschleuse mit mehrstufigem Zugangskontrollsystem
  - Videoüberwachung des Eingangsbereichs, aller Korridore und der Datenverarbeitungsräume
  - Manuelle Schließsysteme (Versperrte Server-Schränke)
  - Dritte werden nur auftrags-/projektbezogen in Begleitung von Mitarbeitern tätig
  - Protokollierung der Besucher

- **Zugangskontrolle**
  Maßnahmen, um die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern:
  - Ausschließlich kabelbasierte Netzwerke (kein WLAN)
  - Aktivitäts-Überwachung (inkl. Alarmierung) nicht genutzter Netzwerk-Schnittstellen
  - Nicht genutzte Schnittstellen von Serversystemen (z.B. USB Ports) sind deaktiviert
  - Betrieb und laufende Weiterentwicklung von Firewalls
  - Dokumentierte Vergaberichtlinie für Benutzer-IDs und Schlüssel/Kennwörter
  - Zugang zu Datenverarbeitungssystemen mit persönlicher Benutzerkennung und privatem Schlüssel oder sicherem Passwort
  - Branchenübliche Kennwort Richtlinien
  - Protokollierung der Logins und fehlgeschlagener Logins
  - Automatische Sperrung von Benutzern

- **Zugriffskontrolle**
  Maßnahmen, um sicherzustellen, dass jeder für die Datenverarbeitungssysteme berechtigte Benutzer ausschließlich auf die ihm berechtigten Daten zugreifen kann und personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
  - Verwendung von Standard Berechtigungsprofilen (Benutzergruppen/Rollen)
  - Eigene Zugänge für Applikationen
  - Regelmäßige anlasslose Überprüfung und Aktualisierung der Berechtigungen
  - Einzelüberprüfungen und Aktualisierungen in Anlassfällen (z.B. Abteilungswechsel eines Mitarbeiters)
  - Standardprozedere bei Ausscheiden von Mitarbeitern

- **Trennung**
  Maßnahmen, um sicherzustellen, dass Daten, welche zu unterschiedlichen Zwecken erhoben wurden, getrennt gespeichert werden.
  - Logische Kundentrennung (softwareseitig)
  - Trennung durch eigene System-/FTP-Benutzer
  - Separation der Daten unterschiedlicher Kunden in getrennten Verzeichnissen (Shared Webhosting- und Shared E-Mail-Hosting-Dienstleistungen) und auf eigenen Partitionen (virtuelle Server).

2. Integrität gemäß Art. 32 Abs. 1 lit. b DSGVO

- **Weitergabekontrolle**
  Maßnahmen, um sicherzustellen, dass personenbezogene Daten bei elektronischer Übertragung oder Speicherung sowie beim Transport der Datenträger nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Abhängig vom Projekt):
  - Zugang über VPN
  - Nutzung von Verbindungsverschlüsselung bei Systemübergängen
  - Führung einer Inventarliste zu externen Speichermedien und kontrollierte Datenträgervernichtung
- **Eingabekontrolle**
  Maßnahmen um sicherzustellen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, bearbeitet und entfernt worden sind:
  - Protokollierung (inkl. regelmäßiger Auswertung) von Verbindungsdaten/Zugriffen bei Shared Webhosting- und Shared E-Mail-Server-Dienstleistungen
  - Protokollierung (inkl. regelmäßiger Auswertung) von Arbeiten bei System-Operating und Unterstützungs-Dienstleistungen (Transfer von Website-Inhalten und Datenbanken von Drittanbietersystemen)
  - Protokollierung (inkl. Auswertung) bei der Übernahme von Mailbox-Inhalten von Drittanbietersystemen
  - Regelungen zum Zugriff auf Protokolle und zur Löschung von Protokollen
- **Systemsicherheit**
  - Betrieb von Virenscannern und weiterer Software zur Schadsoftware-Erkennung
  - Nutzung von Firewalls und Intrusion Detection Systemen
  - Regelmäßige Sicherheitsprüfungen auf Infrastruktur- und Anwendungsebene
- **Softwaresicherheit**
  - Bei Shared Webhosting Dienstleistungen und Managed-Servern übernimmt der Auftragnehmer die laufende Wartung des Betriebssystems und der damit verbundenen Basis-Software (z.B. Systembibliotheken).
  - Bei Shared Webhosting-Dienstleistungen werden Skriptsprachen und Datenbanktechnologien in aktuellen (vom Hersteller gepflegten) Fassungen zur Verfügung gestellt. Die Auswahl aktueller Skriptsprachen und Datenbanktechnologien und die Verwendung aktueller Versionen der Anwendungssoftware (CMS, Onlineshop-, Blog-Systeme, etc.) und deren regelmäßige Wartung obliegen dem Verantwortlichen/Webmaster.

3. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

- **Verfügbarkeit**
  Maßnahmen, um sicherzustellen, dass personenbezogene Daten vor zufälliger oder mutwilliger Zerstörung und Verlust geschützt sind:
  - Schutzmaßnahmen Serverbetrieb in den Datencentern (Interxion 1210 Wien und CenturyLink 81829 München):
    - USV (unterbrechungsfreie Stromversorgung)
    - Überspannungsschutz
    - Idealtemperatur-Klimatisierung und Luftentfeuchtung
    - Schutz gegen Feuer und Wassereintritt
  - Redundante Netzwerk- und Server-Infrastruktur
  - Spiegelung von Festplatten (Festplattenspeicher im RAID-Verbund)
  - Automatisierte Spiegelung aller Daten von Shared Webosting- und Shared E-Mail-Server-Dienstleistungen
  - Monitoring aller Server-Systeme durch internes und externes Monitoring
  - Ersatzteile für Komponenten mit hoher und sehr hoher Ausfallwahrscheinlichkeit vor Ort lagernd
- **Belastbarkeit**
  - Vorhalten von Reservekapazitäten um Hardwareschäden zu kompensieren (Betrieb gespiegelter Systeme)
  - Vorhalten von Ersatz-Hardware um bei Hardwareschäden einen Notfallbetrieb zu gewährleisten (VServer)
  - Robuste Notfallpläne mit laufender Evaluierung
- **Wiederherstellbarkeit (Backup- und Recovery-Konzept)**
  - Regelmäßige Erstellung von Backups
  - Regelmäßige Prüfung der Wiederherstellbarkeit von Backups
  - Definition von Löschfristen für Backupdaten

Tel.: +49 8654 4042002
FAX: +43 6215 20889
support@alldomains.hosting
www.alldomains.hosting

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Auftragskontrolle**
  Maßnahmen, um sicherzustellen, dass personenbezogene Daten nur auf Weisung des Auftraggebers verarbeitet werden können:
  - Zwischen Auftragnehmer und eventuellen Subauftragnehmern werden bei Bedarf Auftragsdatenverarbeitungs-Verträge geschlossen.
- **Datenschutz-Management**
  - Es sind ein Datenschutz-Koordinator und ein stellvertretender Datenschutz-Koordinator benannt
  - Die Kontaktdaten der Datenschutz-Koordinatoren sind öffentlich zugänglich
  - Mitarbeiter werden regelmäßig geschult
- **Incident-Response-Management**
  Ein organisatorischer und technischer Vorgang im Falle eines Sicherheitsvorfalls ist definiert und implementiert. Im Rahmen solcher Fälle erfolgt eine Nachbearbeitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.
  - Die Benachrichtigung des Auftraggebers durch den Auftragnehmer erfolgt automatisiert (Fund von Schadsoftware bei Shared Webhosting-Dienstleistungen, Missbrauch von Shared E-Mail-Server-Dienstleistungen).
  - Die Benachrichtigung des Auftraggebers durch den Auftragnehmer erfolgt unverzüglich manuell bei allen anderen Vorfällen.
  - Alle Vorfälle werden dokumentiert und regelmäßig ausgewertet.
- **Datenschutzfreundliche Voreinstellungen**
  Es ist sichergestellt, dass technisch-organisatorische Maßnahmen getroffen sind, welche dem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Sinne des Art. 25 Abs. 2 DSGVO entsprechen:
  - Die Erfassung von Log-Aufzeichnungen erfolgt ausschließlich in anonymisierter Form. Eine Änderung des Log-Formats hin zu einer Aufzeichnung personalisierter Daten ist nicht vorgesehen.
  - Verzeichnisinhalte werden von Webservern standardmäßig nicht gelistet (DirectoryListing). Eine Änderung der Konfiguration ist durch den Auftraggeber möglich.
  - Shared Webhosting- und VServer-Dienstleistungen weisen zum Zeitpunkt der Einrichtung die aktuellsten verfügbaren Software-Versionsstände auf.
  - Verbindungsverschlüsselung (SSL/TLS) steht bei Shared Webhosting-Dienstleistungen kostenfrei zur Verfügung (Let's Encrypt).
  - Der Zugriff auf Mailbox-Inhalte ist bei Shared E-Mail-Server- und Shared Webhosting-Dienstleistungen ausschließlich bei aktiver Übertragungsverschlüsselung möglich.
- **Regelmäßige Evaluierung**
  - Die Datenschutz-Agenden werden von den Zuständigen regelmäßig überprüft, evaluiert und angepasst.
  - Technische und organisatorische Maßnahmen werden laufend weiterentwickelt.
  - Der Auftragnehmer plant, regelmäßig Auftraggeber aktiv einzuladen um deren Bedürfnisse, Ansichten, Standpunkte und Sichtweisen bei der regelmäßigen Evaluierung einfließen zu lassen.

5. Subunternehmer

Zurzeit sind für den Auftragsverarbeiter keine Subunternehmer zur Verarbeitung personenbezogener Daten tätig.

6. Änderungshistorie dieses Dokuments (Changelog)

2018-05-11: Ursprungsfassung

2019-11-27: Erweiterung Punkt 3. (Verfügbarkeit) um zusätzlichen Datencenter-Standort (München/BRD)