InterDomain

Vereinbarung

über eine

Auftragsverarbeitung nach Artikel 28 DSGVO

Der Auftragsverarbeiter:

InterDomain Software u. IT Consulting GmbH
Khuenstraße 26
3040 Neulengbach

(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieser Vereinbarung ist die Durchführung folgender Aufgaben:

- virtuelle Server Hosting
- Terminalserver
- eMail Hosting – Microsoft Exchange
- Virtuelles Desktop Hosting – VDI
- ESET® Managed Security
- Webseiten Hosting – Webspace oder Webserver
- PRTG Monitoring Server Hosting
- Datensicherung mit Veeam Backup & Replikation, Veeam Backup Agent für Windows und Veeam Cloud Connect
- Disaster Recovery – Backup und virtuelle Server Hosting
- Datensicherung mit AustrianVault Backup
- 3CX VOIP Server
- MailStore Mailarchivierung
- Enterprise LoadBalancing

(2) Folgende Datenkategorien werden verarbeitet, gespeichert oder gesichert:

Kontaktdaten
Vertragsdaten
Verrechnungsdaten
Bonitätsdaten
Personendaten
Bestelldaten
Buchhaltungsdaten
Gehalts und Lohndaten
Mitarbeiterdaten
Angebotsdaten
Patientendaten
Rezeptdaten
Sozialversicherungsdaten
Sonstige Daten

(3) Folgende Kategorien betroffener Personendaten werden Verarbeitet:
Privatpersonen
Firmenkunden
Interessenten
Lieferanten
Ansprechpartner
Mitarbeiter
Patienten

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 3 Monaten 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 Artikel 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 Artikel 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 Artikel 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle 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 oder 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 Europäischen Union oder der Mitgliedstaaten.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb Österreichs durchgeführt.

Anlage 1 – Technisch-organisatorische Maßnahmen

VERTRAULICHKEIT

- **Zutrittskontrolle:** Alle Datenverarbeitungsanlagen befinden sich in gesicherten Räumlichkeiten welche durch Chipkarten, elektrische Türöffner, Sicherheitsschleusen, 24*7 Sicherheitspersonal, Alarmanalgen und Videoüberwachung geschützt sind. Jeder Zutritt wird elektronisch protokolliert und aufgezeichnet.

- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, durch Intrusion Prävention System, automatische Sperrmechanismen, Kennwort Policy und wenn möglich AES Verschlüsselung der Daten.

- **Zugriffskontrolle**: Es ist 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 durch Dritte möglich.

- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung mit AES verschlüsselt und anonymisiert.

INTEGRITÄT[1]

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, Virtual Private Networks (VPN) oder elektronischer Signatur;

- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch Protokollierung.

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Brandschutzanlagen, Löschanlagen,

[1] Verhinderung von unbeabsichtigter Zerstörung/Vernichtung, unbeabsichtigter Schädigung, unbeabsichtigtem Verlust, unbeabsichtigter Veränderung von personenbezogenen Daten.

Virenschutz, Intrusion Prävention Systeme, redundante Firewalls, 24*7 Monitoring, Security Checks auf Infrastruktur- und Applikationsebene, Backupkonzept, Standardprozesse bei Wechsel und Ausscheiden von Mitarbeitern;

- Rasche **Wiederherstellbarkeit**;

- **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles und dergleichen.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen.

- Incident-Response-Management.

- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Artikel 28 DSGVO ohne entsprechende schriftliche Weisung des Auftraggebers.