Anlage 1
Technische organisatorische Maßnahmen

Die Server zur Leistungserbringung der goneo Internet GmbH (Auftragnehmer) befinden sich im Rechenzentrum des Dienstleisters MK Netzdienste GmbH & Co. KG in Frankfurt am Main. Das Rechenzentrum ist zertifiziert nach TÜV „Trusted Site Infrastructure".

Beim Auftragnehmer und dem Dienstleister MK-Netzdienste sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Das Zutrittskontrollsystem (Türöffnung) zum Rechenzentrum besteht aus einer Zwei-Phasen-Autorisierung mit Protokollierung.

Eingangs- und Sicherheitsbereiche werden videoüberwacht mit einer kurzzeitigen Aufzeichnung. Das Gebäude ist alarmgesichert.

1.2 Zugangskontrolle

Der Zugang zu den Serversystemen für administrative Zwecke erfolgt über Benutzername / Kennwort innerhalb eines abgeschotteten Netzwerkes.

Beim automatischen, erstmaligen Erstellen von Zugangsdaten und auch beim manuellen Setzen von neuen Kennwörtern wird auf Kennwortsicherheit geachtet.

Für Kunden existieren Zugangsmöglichkeiten über Benutzername und Kennwort, um Webspace, Mail-Accounts und Datenbanken zu pflegen. Kennwörter werden dabei nicht im Klartext gespeichert.

1.3 Zugriffskontrolle

Es existieren unterschiedliche Berechtigungen gemäß den unterschiedlichen administrativen Aufgaben.

Kunden haben nur Zugriff auf ihre eigenen, der Leistungsbeschreibung entsprechenden Bereiche wie Webspace, E-Mail-Accounts und Datenbanken und ihren Daten und Einstellmöglichkeiten im Kundenportal.

Die Zugriffe werden über Log-Dateien protokolliert.

1.4 Trennungskontrolle

Entwicklungs-, Test- und Live-Systeme sind getrennt eingerichtet.

2 Verschlüsselung

Der Zugang zu den Serversystemen für administrative Zwecke erfolgt über verschlüsselte Verbindungen und innerhalb eines abgeschotteten, internen Netzwerkes.

Für Kunden existieren verschlüsselte Zugriffmöglichkeiten auf ihre Bereiche wie Webspace, E-Mail-Accounts und Datenbanken, sowie das Kundenportal.

3 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Weitergabekontrolle

Die Weitergabe von Daten an Dienstleister zur Auftragserfüllung erfolgt in verschlüsselter Form über verifizierte Kommunikationswege.

3.2 Eingabekontrolle

Protokolliert werden Änderungen, die der Kunde über das Kundenportal durchführt. Änderungen, die Support-Mitarbeiter auf Kundenwunsch durchführen, werden in einem Ticket-System protokolliert.

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.1 Verfügbarkeitskontrolle

- Es werden tägliche Backups der Daten in den verschiedenen Bereichen durchgeführt.
- Server sind mit redundanten Festplattensystemen und Netzteilen ausgestattet.
- Mail- und DNS-Server sind redundant vorhanden.
- Das Rechenzentrum ist mit einer unterbrechungsfreien Stromversorgung, Notstromaggregat und einem Feuermelde / -löschsystem ausgestattet.
- Server und Dienste sind durch Firewalls geschützt und werden überwacht. Bei Ausfall oder Überlastung erfolgt eine automatische Meldung an die zuständigen Mitarbeiter.
- Systeme zur automatischen Erkennung und Verhinderung von Angriffen auf Dienste und Authentifizierungssysteme sind vorhanden.

4.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Das Wiederherstellen von Backups wird regelmäßig getestet.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Der Auftragnehmer prüft seine geltenden technisch-organisatorischen Maßnahmen in regelmäßigen Abständen, mindestens jährlich auf ihre Wirksamkeit und Angemessenheit. Falls notwendig, passt er sie an veränderte Anforderungen sowie den Stand der Technik an.

Die Kompetenzen zwischen Auftraggeber und Auftragnehmer werden bei Datenverarbeitungsverträgen mittels folgender Maßnahmen abgegrenzt:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Online-Bestellsystem)
- Kontrolle der Vertragsausführung