Anlage B: Technische und organisatorische Maßnahmen zum Datenschutz

gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO

1. Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:
Authentifizierung per E-Mail Adresse und Passwortvergabe.

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:
Zugriffseinschränkung durch Accountvergabe.

1.3 Zugriffskontrolle

Es ist sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:
Regelung durch Masterzugang, Einschränkung des jeweiligen Kundenkontos (jedes Kundenkonto kann lediglich die eigenen Daten einsehen).

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:
Zugangsdaten werden via E-Mail mit SSL-Schlüssel übertragen und der Server erfordert eine Authentifizierung des versendenden Accounts.
Passwörter werden gesondert übermittelt.
Der Kunde wird dazu angehalten, das Passwort in regelmäßigen Abständen zu ändern.

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:
-entfällt-

1.6 Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne

Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Beim Auftragnehmer umgesetzte Maßnahmen:
Verschleierung des Weblogins.
Anderenfalls: -entfällt-

1.7 Verschlüsselung
Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Durch den Auftragnehmer umgesetzte Maßnahmen:
Serverfirewall, Accountchiffrierung.

2. Integrität

2.1 Eingabekontrolle
Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:
Nachvollziehbar durch Logfileprotokolle.

2.2 Weitergabekontrolle
Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle
Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:
Mehrfache Backups und Sicherung der Backups.

3.2 Rasche Wiederherstellbarkeit
Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Durch den Auftragsnehmer umgesetzte Maßnahmen:
Wiederherstellung durch regelmäßige Einrichtung von Wiederherstellungspunkten auf Masteraccount.

4. Weitere Maßnahmenbereiche

4.1 Datenschutz-Managementsystem
Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

Beim Auftragnehmer umgesetzte Maßnahmen:

99,9 prozentige Gewährleistung der Sicherheitseinstellung des Servers durch administrative Tätigkeit der Firma Mittwald.

4.2 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:
Eine Verwendung der personenbezogenen Daten über den Auftrag hinaus bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers, ebenfalls kann der Auftraggeber auf eine Verschwiegenheitserklärung der personenbezogenen Daten bestehen.