Anlage B: Technische und organisatorische Maßnahmen zum Datenschutz

gemäß Artt. 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 Hosting-Leistung genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Das Betriebsgebäude ist in unterschiedliche Zutrittsbereiche eingeteilt.
- Besucher melden sich am Empfang und werden vom Ansprechpartner abgeholt.
- Der Zutritt zu sämtlichen Datenverarbeitungsanlagen ist Unbefugten vollständig verwehrt.
- Der Zutritt jeglicher Personen (auch Mitarbeiter) muss durch autorisiertes Personal im Voraus genehmigt werden und wird durch eine Personenkontrolle überprüft.
- Sämtliche Zugänge und Räumlichkeiten der Datenverarbeitungsanlagen werden durch Kameras überwacht und durch elektronische Schließsysteme kontrolliert.
- Jeglicher Zutritt wird protokolliert.

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:

- Zugang zu den Datenverarbeitungsanlagen erhält ausschließlich autorisiertes und fachlich qualifiziertes Personal.
- Der Zugang erfolgt über eine Benutzerkennung und Eingabe eines Passwortes.
- Die Passwörter entsprechen einem technisch sicheren Niveau und sind durch interne Richtlinien geregelt.
- Die Anmeldungen werden protokolliert.

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:

- Der Zugriff auf die Datenverarbeitungssysteme ist durch eine Nutzer- und Rechteverwaltung abgesichert. Es ist dem einzelnen Mitarbeiter nur möglich die für seine Aufgaben erforderlichen Daten einzusehen, zu nutzen, zu verarbeiten oder zu löschen.
- Die Zugriffe auf die Datenverarbeitungssysteme werden geloggt.
- Beim Verlassen des Arbeitsplatzes erfolgt eine Sperrung durch Bildschirmschoner, Freigabe nur durch Eingabe des Passworts.
- Jeder Mitarbeiter wird entsprechend zur Vertraulichkeit und der Einhaltung des Datenschutzes bei Aufnahme seiner Tätigkeit verpflichtet. Ein Verstoß hätte die fristlose Kündigung, sowie eine Strafanzeige zur Folge. Betroffene Auftraggeber würden in so einem Fall selbstverständlich über den Vorfall informiert.

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:

- Der Auftragnehmer überträgt von sich aus personenbezogene Daten ausschließlich elektronisch über verschlüsselte Datenverbindungen, so dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Eine elektronische Übertragung personenbezogener Daten erfolgt ausschließlich im Rahmen des Bestellprozesses, dem Abruf von Kundendaten im Servicefall, innerhalb des Mahnverfahrens, zur Registrierung von Domains und SSL Zertifikaten, und zur Datensicherung der Kundenumgebungen.
- Erhebt, verarbeitet oder nutzt ein Kunde im Rahmen des Hostingvertrages personenbezogene Daten, so obliegt die Absicherung der Datenübertragung (z.B. über HTTPS) seiner Verantwortung.
- Nicht mehr benötigte oder defekte Datenträger werden durch ein zertifiziertes Unternehmen entsorgt.

1.5 Trennungskontrolle

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

Beim Auftragnehmer umgesetzte Maßnahmen:

- Es gibt je nach gewähltem Hostingmodell mindestens eine logische (virtuelle) Mandantentrennung.
- Es obliegt der Verantwortung des Kunden innerhalb seiner Kundenumgebung sicher zu stellen, dass dieses in gleichem Maß für von Ihm erhobene personenbezogene Daten gilt.

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:

- Die Pseudonymisierung personenbezogener Daten im

Rahmen des Hostingvertrages und der dort vom Auftraggeber betriebenen Anwendungen obliegt dem Auftraggeber.

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:
- Verschlüsselte Datenübertragung (verschlüsselte Internetverbindungen mittels TLS/SSL).

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:
- Die Eingabe, Änderung oder Löschung personenbezogener Daten, die im Verantwortungsbereich der Mittwald CM Service GmbH & Co KG liegen, werden mit der Kennung des zuständigen Mitarbeiters geloggt.
- Erhebt, verarbeitet oder nutzt ein Kunde im Rahmen des Hostingvertrages personenbezogene Daten, so obliegt es seiner Verantwortung entsprechende Loggingmechanismen für seine Webumgebung zu implementieren.

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:
- Soweit es technisch möglich ist, sind sämtliche auf Datenverarbeitungssystemen der Mittwald CM Service GmbH & Co KG liegenden Daten im Rahmen der Ausfallsicherheit vor zufälligem Verlust oder Zerstörung geschützt.
- Hierzu kommen u.a. RAID Systeme, Ersatzhardware, Überspannungsschutz, USV-Anlagen, Notstromaggregat, Löschgasanlage zum Einsatz.
- Weitergehend wird mindestens ein Backup des Vortages (tarifabhängig) bereitgehalten.

Beim Produkt Root-Server findet keinerlei Backup statt, der Auftraggeber muss selbst für eine geeignete Datensicherung sorgen.

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:
- IT-Notfallpläne und Wiederanlaufpläne
- Regelmäßige und dokumentierte Datenwiederherstellungen

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:
- Managementsystem zum Datenschutz und der Informationssicherheit
- Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
- Durchführung regelmäßiger IT-Schwachstellenanalysen
- Durchführung regelmäßiger interner Audits
- Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen

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:
- Personenbezogene Daten werden von der Mittwald CM Service GmbH & Co KG nur im Rahmen des Bestellprozesses, sowie bei Logging von Verbindungsdaten (IP-Adressen) erhoben, verarbeitet und genutzt.
- Von Kunden erhobene personenbezogene Daten werden ausschließlich im Servicefall im Auftrag des Kunden verarbeitet (Erstellung und Wiederherstellung eines Backups, Reparatur der Kundendatenbank, o.ä.).
- Für den Umgang mit Kundendaten werden nur die unter www.mittwald.de/unsere-dienstleister genannten Unterauftragnehmer als externe Dienstleister eingesetzt.