Technische und organisatorische Maßnahmen

The New Crispy Mountain GmbH

Stand: 01. Oktober 2026

Präambel

The New Crispy Mountain GmbH („**Anbieter**“) mit Sitz in Mainz, Deutschland bietet eine webbasierte Software-as-a-Service (SaaS) Plattform für Druckereien namens Keyline („**Keyline**“) und damit verbundene Services („**Services**“) für Unternehmen an („**Kunden**“).

Der Anbieter versteht sich als modernes und vollständig digitales Unternehmen, das großen Wert auf Datenschutzbestimmungen und sorgsame Datenverarbeitung legt.

Die folgende Auflistung beschreibt die technischen und organisatorischen Maßnahmen, um dies sicherzustellen (gem. Art. 32 DSGVO).

1. Zutrittskontrolle

1.1. Der Anbieter ist eine so genannte “remote company”. Das bedeutet, dass nahezu alle Mitarbeitenden nicht am Firmenstandort in Mainz ansässig sind. Entsprechend ist der physische Zutritt zu den Büroräumen in Mainz von nachrangiger Bedeutung.

1.2. Der Anbieter betreibt am Standort in Mainz keine Server. Alle Mitarbeitenden verfügen über Laptops, iPads und Smartphones, die im Büro nicht unbeaufsichtigt zurückgelassen werden.

1.3. In den Büroräumen des Anbieters befinden sich nur in geringen Mengen Papierunterlagen, da der Anbieter nahezu ausschließlich papierlose Prozesse verwenden.

1.4. Der Zutritt zu den Büroräumen ist nur mit individuell an Mitarbeitende herausgegebene Schlüssel möglich. Die Aus- und Rückgabe von Schlüsseln wird in einem Schlüsselplan protokolliert. Es gibt definierte Regelung zum Verschließen der Zugangstüren und -fenster beim Verlassen der Büroräume, Zugang von Fremdpersonal nur nach Vorabprüfung und/oder in Begleitung von autorisierten Mitarbeitern, Aufenthalt von Besuchern nur in Begleitung von autorisierten Mitarbeitern.

1.5. Alle Mitarbeitenden, die von zu Hause aus arbeiten, sind angehalten die IT-Geräte des Anbieters sicher zu verwahren. Gleiche Regelungen gelten beim Nutzen von Co-Working Einrichtungen. Weniger mobile Geräte dürfen grundsätzlich nur kurzzeitig unbeaufsichtigt gelassen werden, und auch nur wenn eine Sperrung des Gerätes erfolgt ist (beispielsweise Schließen des Laptops, Bildschirmsperre u.ä.). Mobile Geräte dürfen grundsätzlich nicht unbeaufsichtigt zurückgelassen werden.

2. Zugangskontrolle

2.1. Alle Computer, Tablets und Smartphones der Mitarbeitenden des Anbieters sind mit Benutzername und Passwort bzw. PIN Code geschützt. Bei Smartphones werden außerdem biometrische Verfahren zur Zugangskontrolle eingesetzt (FaceID bzw. Fingerprint).

2.2. Alle Geräte sind über ein MDM fernwartbar und identifizierbar. Der Standort jedes Gerätes kann bei Verlust oder Diebstahl jederzeit ermittelt werden und ggf. die Löschung des Gerätes in die Wege geleitet werden.

2.3. Die Mitarbeiter sind angehalten, einen Passwort-Manager zu verwenden, der für jeden Zugang sichere Passwörter generiert und speichert. Der Zugriff auf dieser Passwort-Manager erfolgt im Multifaktor-Verfahren (MFA).

2.4. Die Mitarbeiter sind angehalten, eine „Clean Desk Policy“ einzuhalten. Das bedeutet, dass keine Dokumente, Unterlagen und Notizen unbeaufsichtigt am Arbeitsplatz hinterlassen werden.

3. Zugriffskontrolle

3.1. Der Anbieter nutzt standardisierte und zentralisierte Verfahren zur Vergabe von Benutzerkennungen und Berechtigungen mit definierten Freigaben sowohl für unternehmensinterne Benutzer als auch für externe Benutzer unter Verwendung unterschiedlicher Daten-Tresore im Passwort-Manager-Tool.

3.2. Als Kernbestandteil eines mehrstufigen Sicherheitskonzeptes erhalten Mitarbeitende Zugriff auf Datenverarbeitungsdienste nach dem "need to know"-Prinzip. Obwohl dies einen größeren administrativen Aufwand verursacht, stellt der Anbieter so sicher, dass jede Person nur Zugriff auf die zur Erfüllung ihrer jeweiligen Tätigkeit notwendigen Daten erhält. Somit wird die jeweilige Angriffsfläche pro Mitarbeitendem verringert (Containment-Strategie). Dies trifft auch auf Entwickler und technische Mitarbeitende zu.

3.3. Grundsätzlich werden Zugriffe auf alle kritischen Anwendungen protokolliert, insbesondere bei der Eingabe, Änderung und Löschung von Daten.

3.4. Die datenschutzkonforme Löschung und Vernichtung von Datenträgern (Akten, Laufwerke etc.) wird eingehalten.

3.5. Der Anbieter verschlüsselt die Datenträger aller im Umlauf befindlichen Endgeräte.

4. Trennungskontrolle

4.1. Der Anbieter stellt auf Applikationsebene sicher, dass, nach den aktuellen technischen Möglichkeiten, Daten unterschiedlicher Mandaten getrennt sind.

4.2. Systeme werden bereits auf Infrastrukturebene in Staging, Sandbox und Produktiv-Systeme getrennt. In den Staging und Sandbox-System werden keinerlei Kundendaten gespeichert.

4.3. In der Regel werden keine Daten aus dem Produktivsystem auf lokale Computer heruntergeladen. Wenn Produktivdaten zur Fehlersuche benötigt werden, so wird versucht diese soweit möglich zu anonymisieren. Nur in Ausnahmefällen weicht der Anbieter von dieser Praxis ab. Unabhängig davon sind alle Daten im gesamten Transportprozess und anschließend auf den Endgeräten durchgehend verschlüsselt.

4.4. Zugriffe auf Applikationen und Datenbanken sind über ein Berechtigungskonzept nach dem „Need to know“ Prinzip verteilt, so dass nur diejenigen Personen Zugriff auf diese Systeme haben, die diesen wirklich haben müssen.

5. Weitergabekontrolle

5.1. Alle Daten werden bei der netzwerkbasierten Übertragung transportverschlüsselt (HTTPS, SSL/TLS, SSH). Der Anbieter nutzt keine Dienste bei denen dies nicht gewährleistet wäre. Alle zur Verfügung gestellten Dienste können nur per HTTPS angesprochen werden.

5.2. Alle Mitarbeitenden unterliegen organisatorischen und technischen Anweisungen zur Aufbewahrung, Weitergabe und Löschung von Daten gemäß den Vorgaben der Informationssicherheits- und Datenschutzrichtlinie.

5.3. Alle Mitarbeitenden werden regelmäßig im Bereich Informationssicherheit und Cybersecurity geschult.

5.4. Der Anbieter prüft die Sicherheit seiner Systeme, Prozesse und die Sensibilität seiner Mitarbeitenden regelmäßig im Rahmen von Penetration Tests, bei denen auch auf unangekündigte social engineering Methoden zurück gegriffen wird.

6. Eingangskontrolle

6.1. Alle Erfassungen, Änderung und Löschung von kritischen Daten werden über die in den jeweiligen Anwendungssystemen integrierten Logs protokolliert.

6.2. Der Anbieter überprüft regelmäßig die Berechtigungskonzepte der Benutzer und die ordnungsgemäße Vergabe von Berechtigungen im Rahmen von regelmäßigen Audits.

7. Verfügbarkeitskontrolle

7.1. Der Anbieter führt gemeinsam mit seinen Infrastrukturanbietern in einem mehrstufigen Konzept regelmäßig Datensicherungen durch.

7.2. Alle Produktivsysteme werden im "hot-failover" Modus betrieben, sodass auch bei Ausfällen in der Regel ein reibungsloser Weiterbetrieb sichergestellt ist.

7.3. Der Anbieter besitzt keine eigenen Server oder (Netzwerk)-Infrastruktur, sondern nutzt Service Provider für Server, Speicher und Netzwerkressourcen und sonstige IT-Infrastruktur. Somit besteht keine Gefahr eines Ausfalls oder Datenverlustes durch Unfälle am Unternehmensstandort.

7.4. Das IT-Team des Anbieters ist 24 Stunden/365 Tage in Bereitschaft um technische Störungen rasch zu beheben oder Angriffe abzuwehren. Dabei werden automatisierte Alarmierungen und ein mehrstufiges Response-Konzept eingesetzt.

7.5. Das technische Personal des Anbieters übt regelmäßig ein potentielles (Neu-) Aufsetzen der Infrastruktur und das Einspielen von Backups.

7.6. Sämtliche Systeme werden automatisiert und in Echtzeit auf Verfügbarkeit und Performance überwacht. Kritische Systeme werden zusätzlich automatisiert auf verdächtige Aktivitäten hin überwacht.