

FÜR GESCHÄFTSKUNDEN (B2B)

Vereinbarung zur Auftragsverarbeitung

für den H5M Sicherheitscheck für Microsoft 365 („AVV Sicherheitscheck“) nach Art. 28 DSGVO

High5Manufaktur GmbH

Am Buchenhain 2, 76359 Marxzell · h5m.de

Fassung 1.0 · Stand: 29.09.2026

Vertragstext für Bestellungen über h5m.de, mit den Anlagen 1 bis 3

Vereinbarung zur Auftragsverarbeitung

für den H5M Sicherheitscheck für Microsoft 365 („AVV Sicherheitscheck“) nach Art. 28 DSGVO

High5Manufaktur GmbH, Am Buchenhain 2, 76359 Marxzell · Fassung 1.0 · Stand: 29.09.2026

Zwischen dem in der Bestellung genannten Kunden („Verantwortlicher“) und der High5Manufaktur GmbH, Am Buchenhain 2, 76359 Marxzell, vertreten durch den Geschäftsführer Alexander Häffner („H5M“). „Bestellung“ meint die Bestellung des Sicherheitschecks über die Website h5m.de oder über eine Bestellseite der H5M nach § 1 Abs. 1 der Ergänzenden Bedingungen, „Bestelladresse“ die dabei angegebene E-Mail-Adresse. Mit dem Abschluss des Bezahlvorgangs gibt der Kunde sein Angebot auf Abschluss des Vertrags über den Sicherheitscheck einschließlich dieser Vereinbarung ab (§ 4 Abs. 2 der Ergänzenden Bedingungen). Diese Vereinbarung wird zusammen mit dem Vertrag über den Sicherheitscheck durch die Auftragsbestätigung per E-Mail elektronisch geschlossen (§ 4 Abs. 4 der Ergänzenden Bedingungen, Art. 28 Abs. 9 DSGVO); H5M hält Zeitpunkt, Fassung, Bestellnummer und bestellende Person fest. Daten aus dem Tenant verarbeitet H5M erst nach der Freigabe (§ 6 der Ergänzenden Bedingungen).

§ 1 Gegenstand und Dauer

- (1) Gegenstand ist die Verarbeitung personenbezogener Daten bei der Erbringung des Sicherheitschecks nach den Ergänzenden Bedingungen. Das umfasst die Prüfung der Freigabe (Anmeldung und Rolle der zustimmenden Person), den lesenden Abruf von Verzeichnis- und Konfigurationsdaten aus dem Microsoft-365-Tenant des Verantwortlichen über die Anwendung „H5M Sicherheitsbericht“, die automatische Auswertung, eine Durchsicht durch den Geschäftsführer vor der Übermittlung zur Qualitätssicherung, soweit H5M sie vornimmt (§ 2 Abs. 1 der Ergänzenden Bedingungen), die Erstellung und Übermittlung des Sicherheitsberichts, Aufbewahrung und Löschung nach § 8, die Bearbeitung von Rückfragen und Fehlern zum Auftrag sowie, falls gebucht, die Durchsprache.
- (2) Die Vereinbarung gilt ab ihrem Abschluss bis zur Löschung nach § 8. Den Tenant ruft H5M nur zwischen der Zustimmung und der Übermittlung des Berichts ab, höchstens bis 14 Tage nach der Zustimmung.

§ 2 Art und Zweck, Daten, betroffene Personen

- (1) Art der Verarbeitung: Abrufen, Auswerten, Zusammenfassen, Speichern, Übermitteln an den Verantwortlichen, Löschen. Bei einer Durchsicht zur Qualitätssicherung (§ 1 Abs. 1) kommen das Ansehen und das Berichtigen der Befunde hinzu, in der Durchsprache das Ansehen von Daten, die der Verantwortliche per Bildschirmfreigabe zeigt.

- (2) Zweck ist ausschließlich die Erbringung des Sicherheitschecks für den Verantwortlichen.
- (3) Datenarten und betroffene Personen nennt Anlage 1. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung.

§ 3 Weisungen

- (1) H5M verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch hinsichtlich Übermittlungen in Drittländer, es sei denn, sie ist nach Unionsrecht oder deutschem Recht dazu verpflichtet. In diesem Fall teilt sie ihm diese Anforderungen vorher mit, sofern das Recht dies nicht verbietet.
- (2) Bestellung, Ergänzende Bedingungen und diese Vereinbarung sind die Weisungen des Verantwortlichen. Weitere Weisungen erteilt er in Textform an datenschutz@h5m.de, von der Bestelladresse oder durch eine vertretungsberechtigte Person. Beispiele sind die vorzeitige Löschung oder die Übernahme der Befunde in einen Betreuungsvertrag mit H5M.
- (3) Hält H5M eine Weisung für datenschutzrechtswidrig, informiert sie den Verantwortlichen unverzüglich (Art. 28 Abs. 3 Unterabsatz 2 DSGVO) und setzt die Ausführung aus. Sie führt die Weisung erst aus, wenn die Bedenken ausgeräumt sind oder der Verantwortliche die Weisung rechtmäßig geändert hat. Die bloße Bestätigung einer weiterhin rechtswidrigen Weisung verpflichtet H5M nicht zu ihrer Ausführung.
- (4) H5M verarbeitet die Daten nicht für eigene Zwecke. Ausgeschlossen sind insbesondere Werbung und Vertrieb, Profilbildung, statistische Auswertungen auch in anonymisierter Form, die Weitergabe an Dritte außerhalb von § 6 und die Übergabe an KI-Sprachmodelle.

§ 4 Pflichten von H5M

- (1) H5M setzt nur zur Vertraulichkeit verpflichtete Personen ein (Art. 28 Abs. 3 Satz 2 lit. b, Art. 29 DSGVO). Zugriff auf die Daten hat bei H5M nur der Geschäftsführer.
- (2) H5M trifft die technischen und organisatorischen Maßnahmen nach Anlage 3 (Art. 32 DSGVO). Sie darf sie dem Stand der Technik anpassen, ohne das Schutzniveau zu unterschreiten.
- (3) H5M unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei Anträgen betroffener Personen (Art. 12 bis 22 DSGVO) und bei den Pflichten aus Art. 32 bis 36 DSGVO, soweit Art der Verarbeitung und verfügbare Informationen dies zulassen.
- (4) H5M meldet eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens 24 Stunden nach Kenntnis, per E-Mail an die

Bestelladresse, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie vorliegen. Meldungen an Aufsichtsbehörde und Betroffene nimmt der Verantwortliche vor.

- (5) H5M stellt auf Anfrage alle Informationen bereit, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind. Sie ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer. Der Prüfer muss unabhängig und zur Vertraulichkeit verpflichtet sein. H5M kann einen Prüfer nur aus nachvollziehbaren Gründen der Informationssicherheit oder wegen eines unmittelbaren Interessenkonflikts ablehnen, etwa wenn er für einen Wettbewerber von H5M tätig ist; der Verantwortliche kann dann einen anderen geeigneten Prüfer benennen. Inspektionen vor Ort finden grundsätzlich mit 14 Tagen Vorlauf während der Geschäftszeiten statt, ohne besonderen Anlass höchstens einmal im Kalenderjahr. Bei einer Verletzung des Schutzes personenbezogener Daten, bei begründetem Verdacht auf einen erheblichen Verstoß und auf Verlangen einer zuständigen Aufsichtsbehörde gelten Vorlauf und Begrenzung nicht. Den angemessenen Aufwand einer anlasslosen Inspektion vor Ort kann H5M berechnen; die Vergütung darf die Ausübung des Prüfungsrechts nicht unangemessen erschweren.
- (6) H5M führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO. Datenschutzrechtlicher Ansprechpartner von H5M ist datenschutz@h5m.de, wie in ihrer Datenschutzerklärung angegeben.

§ 5 Rechte betroffener Personen

Wendet sich eine betroffene Person an H5M, leitet H5M das Anliegen unverzüglich an den Verantwortlichen weiter und handelt nur auf dessen Weisung.

§ 6 Unterauftragsverarbeiter

- (1) Der Verantwortliche genehmigt die Unterauftragsverarbeiter nach Anlage 2.
- (2) Er erteilt eine allgemeine Genehmigung für weitere oder andere Unterauftragsverarbeiter. Solange der Sicherheitscheck noch aussteht oder H5M Daten des Verantwortlichen speichert, informiert sie ihn mindestens 30 Tage vor einer Änderung in Textform an die Bestelladresse. Der Verantwortliche kann innerhalb von 14 Tagen nach Zugang aus angemessenen, auf den Schutz personenbezogener Daten bezogenen Gründen widersprechen. Dann setzt H5M den neuen oder geänderten Unterauftragsverarbeiter für seine Daten nicht ein, soweit das technisch möglich ist, und löscht seine Daten sonst vor der Änderung. Ist der Bericht noch nicht übermittelt, kann er den Vertrag kündigen; H5M erstattet dann den gezahlten Preis vollständig. Fordert der Verantwortliche nach § 6 Abs. 9 der Ergänzenden Bedingungen einen neuen Freigabe-Link an, nennt H5M ihm mit dem Link die Änderungen der Anlage 2 seit der Bestellung; für einen Widerspruch gelten die Sätze 3 bis 5 entsprechend.

- (3) H5M erlegt jedem Unterauftragsverarbeiter durch Vertrag oder ein anderes Rechtsinstrument dieselben Datenschutzpflichten auf, die in dieser Vereinbarung festgelegt sind, soweit sie für seine Verarbeitung einschlägig sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet H5M gegenüber dem Verantwortlichen für deren Einhaltung wie für eigenes Handeln.

§ 7 Ort der Verarbeitung

H5M verarbeitet und speichert die Daten auf ihrer Plattform in Deutschland (Hetzner, Falkenstein); Datensicherungen verschlüsselt sie vor dem Verlassen der Plattform. Die Unterauftragsverarbeiter verarbeiten Daten an den in Anlage 2 beschriebenen Orten. Soweit dabei Daten in Drittländer übermittelt werden oder aus Drittländern auf sie zugegriffen wird, etwa im Netz von Cloudflare oder bei Microsoft außerhalb der EU Data Boundary, geschieht das nur unter den Voraussetzungen der Art. 44 ff. DSGVO und auf den in Anlage 2 genannten Grundlagen.

§ 8 Löschung

- (1) Rohdaten, also die aus dem Tenant abgerufenen Daten, löscht H5M mit der Übermittlung des Berichts, spätestens 30 Tage nach dem Abruf.
- (2) Befunde, also das Ergebnis je Prüfpunkt einschließlich der als Beleg genannten Konten, löscht H5M 90 Tage nach Übermittlung des Berichts. Ist eine Durchsprache gebucht, löscht sie die Befunde 30 Tage nach der Durchsprache, spätestens sechs Monate nach Übermittlung. Solange H5M den Bericht nicht übermittelt hat, löscht sie die Befunde, sobald feststeht, dass sie ihn nicht mehr übermittelt, etwa weil der Vertrag über den Sicherheitscheck endet, spätestens am Tag nach Ablauf von 90 Tagen nach dem Abruf, bei einer Rückfrage nach § 7 Abs. 4 der Ergänzenden Bedingungen am Tag nach Ablauf von 90 Tagen nach deren Versand; bis dahin kann der Kunde die Rückfrage bestätigen. Auf Weisung löscht sie früher.
- (3) Den Bericht speichert H5M nicht; er entsteht bei Bedarf aus den Befunden. Der Link zum Herunterladen gilt 30 Tage.
- (4) Gelöschte Daten verbleiben bis zu 30 Tage in den verschlüsselten Datensicherungen der Plattform und bis zu sieben Tage in den täglichen Abbildern des gesamten Servers beim Hosting-Anbieter und verschwinden mit deren Ablauf. Bis dahin werden sie nur für eine Wiederherstellung verwendet.
- (5) Eigene Unterlagen bewahrt H5M als Verantwortliche auf, soweit Gesetze es verlangen oder sie zum Nachweis nötig sind: Bestellung, Nachweis dieser Vereinbarung und der Freigabe (Zeitpunkte, Kennung des Tenants, Objektkennung und geprüfte Rolle des zustimmenden Kontos, auch im

Protokoll der Plattform), die E-Mails zum Auftrag als Geschäftsbriefe im E-Mail-Archiv, Rechnung und Zahlung. Aus dem Tenant enthalten diese dauerhaft aufzubewahrenden Unterlagen ausschließlich Name, Kennung und Domains des Tenants sowie, soweit zum Nachweis der Freigabe erforderlich, die Objektkennung und die geprüfte Rolle des zustimmenden Kontos. Gesamtbewertung, Zahl der Maßnahmen, einzelne Befunde und Namen betroffener Konten übernimmt H5M weder in E-Mails noch in andere dauerhaft aufzubewahrende Unterlagen.

- (6) Der Verantwortliche weist H5M mit Abschluss dieser Vereinbarung an, Rohdaten und Befunde nach den Absätzen 1 bis 4 zu löschen; die für den Zweck bestimmten Ergebnisse erhält er mit dem Sicherheitsbericht zurück. Bis zur jeweiligen Löschung kann er in Textform statt der Löschung die Rückgabe der bei H5M noch vorhandenen personenbezogenen Daten verlangen, soweit er sie nicht schon mit dem Bericht erhalten hat. Nach einer Rückgabe löscht H5M vorhandene Kopien, soweit keine gesetzliche Pflicht zur Aufbewahrung entgegensteht; für Datensicherungen gilt Abs. 4. Auf Anfrage bestätigt H5M die Löschung in Textform.

§ 9 Haftung

Es gilt Art. 82 DSGVO, im Übrigen § 6 der AGB der H5M.

§ 10 Fassungen

Für jede Bestellung gilt die bei der Bestellung gültige Fassung. Änderungen bedürfen der Textform; für Unterauftragsverarbeiter gilt § 6 Abs. 2.

§ 11 Bestellung durch einen IT-Dienstleister

- (1) Bestellt der Kunde für den Tenant eines von ihm als Auftragsverarbeiter betreuten Unternehmens, bleibt dieses Unternehmen Verantwortlicher, der Kunde ist dessen Auftragsverarbeiter und H5M weiterer Auftragsverarbeiter (Art. 28 Abs. 2 und 4 DSGVO). Diese Vereinbarung gilt dann zwischen Kunde und H5M als Vertrag über die weitere Auftragsverarbeitung. Die Pflichten, die sie H5M gegenüber dem Verantwortlichen zuweist, bestehen in diesem Fall gegenüber dem Kunden in dessen Eigenschaft als Auftragsverarbeiter, soweit dies zur Erfüllung der Pflichten gegenüber dem betreuten Unternehmen erforderlich ist; Weisungen erteilt insoweit der Kunde.
- (2) Der Kunde sichert zu, dass das betreute Unternehmen gesondert oder allgemein schriftlich genehmigt hat, dass H5M als weiterer Auftragsverarbeiter nach Art. 28 Abs. 2 DSGVO eingesetzt wird, und dass etwaige Informations- und Widerspruchspflichten erfüllt sind. Weitergehende Datenschutzpflichten aus seinem Vertrag mit dem betreuten Unternehmen teilt der Kunde H5M vor der Zustimmung, also vor Beginn der Verarbeitung, in Textform mit. H5M

übernimmt die für ihre Verarbeitung einschlägigen Pflichten in Textform; kann sie sie nicht übernehmen, lehnt sie die Bestellung ab und erstattet den gezahlten Preis vollständig. Meldungen nach § 4 Abs. 4 und Informationen nach § 6 Abs. 2 leitet der Kunde unverzüglich an das betreute Unternehmen weiter.

- (3) Eine Bestellung als IT-Dienstleister ist nur zulässig, wenn der Kunde für die betreffende Verarbeitung Auftragsverarbeiter des betreuten Unternehmens ist und H5M als weiteren Auftragsverarbeiter einsetzen darf. Bestellt ein IT-Dienstleister dagegen nur als Vertreter im Namen des betreuten Unternehmens, ist dieses selbst als Kunde und Verantwortlicher anzugeben.

§ 12 Schlussbestimmungen

- (1) In datenschutzrechtlichen Fragen geht diese Vereinbarung den Ergänzenden Bedingungen und den AGB vor.
- (2) Es gilt deutsches Recht. Ist eine Bestimmung unwirksam, bleiben die übrigen wirksam.

Anlage 1: Daten und betroffene Personen

Betroffene: Beschäftigte und sonstige Nutzer mit Konto im Tenant; Administratoren, auch Beschäftigte beauftragter Dienstleister; Gäste (externe Personen); Personen hinter den technischen Kontaktadressen.

Daten:

1. **Konten:** Anzeigename, Anmeldeadresse (UPN), Objektkennung, Mitglied oder Gast, aktiv oder deaktiviert, Erstellungsdatum, ob Lizenz und Postfach vorhanden sind, Postfachtyp, ob das Konto aus einem lokalen Verzeichnis übernommen ist, ob es von den Kennwortregeln ausgenommen ist (nur dieses Merkmal, nie ein Kennwort), bei Gästen der Einladungsstatus.
2. **Rollen:** Mitgliedschaft in Administratorrollen, bei Konten, Gruppen und Anwendungen; bei Gruppen mit Administratorrolle auch die Kennungen ihrer Mitgliedskonten, einschließlich verschachtelter Gruppen (transitiveMembers).
3. **Anmeldesicherheit:** Art der eingerichteten Anmeldemethoden je Konto. Mit Entra ID P1 stammt sie aus dem Registrierungsbericht von Microsoft (Registrierungsstand je Konto, userRegistrationDetails), sonst aus der Abfrage je Konto. Gespeichert wird nur die Art der Methode; von Microsoft mitgelieferte Details wie Telefonnummern oder Gerätenamen werden nur im Arbeitsspeicher verarbeitet. Dazu je Konto der Status der älteren Einstellung „MFA pro Benutzer“.
4. **Ausnahmen von Anmelde Richtlinien:** Kennungen der Konten und Gruppen, die Richtlinien für bedingten Zugriff ausnehmen. Für Richtlinien, die eine zweite Anmeldestufe verlangen, liest der Sicherheitscheck die Mitglieder ausgenommener Gruppen einschließlich verschachtelter Gruppen (Gruppenmitgliedschaften über transitiveMembers) und speichert davon nur die Kennungen der Konten.
5. **Nutzung:** letzte Anmeldung je Konto (mit Entra ID P1) oder, aus dem Nutzungsbericht der letzten 90 Tage, nur das Datum der letzten Aktivität je Konto. Aus den Anmeldeprotokollen der letzten sieben Tage nur das Anmeldeverfahren, ausgewertet als Anzahl je Verfahren. Aus dem Bericht zu Mail-Apps der letzten 90 Tage nur die Zahl der Konten je Protokoll (POP, IMAP, SMTP).
6. **Postfachregeln mit Weiterleitung:** Konto, Name der Regel, Zieldomain, ob aktiv. Vollständige Regeln und Adressen werden nur im Arbeitsspeicher ausgewertet.
7. **Organisation:** Name und Kennung des Tenants, Domains, technische Kontaktadressen, Lizenzen, Richtlinien und Einstellungen zu Anmeldung, Gästen, Gruppen und Freigaben, verbundene Anwendungen mit ihren Rechten und der Angabe, ob einzelne Personen zugestimmt haben (ohne deren Namen), Namen und Ablaufdaten der Geheimnisse und Zertifikate eigener App-Registrierungen (nie die Geheimnisse selbst), Secure Score mit seinen Einzelmaßnahmen, öffentliche DNS-Einträge der Mail-Domains. Personenbezug nur ausnahmsweise.

8. **Freigabe:** Kennung des Tenants, Objektkennung und geprüfte Rolle des Kontos (Anlage 3 Teil B Nr. 2), mit dem sich die zustimmende Person angemeldet hat, Zeitpunkte von Zustimmung, Anmeldung und Rollenprüfung. Name und Anmeldename aus der Anmeldung werden nur im Arbeitsspeicher verarbeitet.
9. **Ergebnis:** Befunde je Prüfpunkt, als Beleg mit einer begrenzten Auswahl betroffener Konten.
10. **Durchsprache:** Daten, die der Verantwortliche per Bildschirmfreigabe zeigt. Er achtet darauf, nur die für die Durchsprache nötigen Einstellungen zu zeigen und keine Inhalte und keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) einzublenden.

Nicht verarbeitet werden Inhalte von E-Mails, Dateien, Chats oder Kalendern, Kennwörter und Geheimnisse.

Anlage 2: Unterauftragsverarbeiter

1. **Hetzner Online GmbH**, Industriestr. 25, 91710 Gunzenhausen: Betrieb der Plattform (Server, Datenbank), Rechenzentrum Falkenstein. Deutschland.
2. **Cloudflare, Inc.**, 101 Townsend St., San Francisco, CA 94107, USA: Netzzugang zur Plattform (Proxy, Tunnel, TLS), Zugriffsschutz, Ablage verschlüsselter Datensicherungen (R2). Globales Netz, eine Beschränkung auf die EU ist nicht zugesichert. Grundlage der Übermittlung in die USA: Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework (Cloudflare ist zertifiziert), hilfsweise die EU-Standardvertragsklauseln 2021/914 aus dem Cloudflare-DPA.
3. **IONOS SE**, Elgendorfer Str. 57, 56410 Montabaur: zweites Sicherungsziel (Object Storage, Rechenzentrum Berlin); Daten aus dem Tenant dort nur in client-seitig verschlüsselten Datenbanksicherungen. Deutschland.
4. **Microsoft Ireland Operations Ltd.**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland: Microsoft 365 der H5M, insbesondere Exchange Online für E-Mails zum Auftrag und Microsoft Teams für die Durchsprache. Die EU Data Boundary ist aktiv. Microsoft beschreibt begrenzte fortbestehende Übermittlungen und Zugriffe außerhalb der EU Data Boundary, unter anderem für Fernzugriffe, Sicherheits- und Betriebszwecke, Verzeichnisdaten und Netzwerktransit. Soweit dabei Daten in Drittländer übermittelt werden, gelten die von Microsoft dafür vorgesehenen Grundlagen nach Art. 44 ff. DSGVO, insbesondere Angemessenheitsbeschlüsse oder EU-Standardvertragsklauseln.
5. **Hornetsecurity GmbH**, Am Listholze 78, 30177 Hannover: E-Mail-Sicherheit und revisionssicheres E-Mail-Archiv der H5M. Deutschland.

Transparenzhinweis: Microsoft als Anbieter des Tenants des Verantwortlichen ist dessen eigener Dienstleister und kein Unterauftragsverarbeiter von H5M. Für eigene Zwecke setzt H5M ohne Zugriff auf Tenant-Daten ein: Stripe Payments Europe, Limited (Zahlung), BuchhaltungsButler GmbH und easybill GmbH (Buchhaltung und Rechnungen).

Anlage 3: Technische und organisatorische Maßnahmen

Teil A: Allgemeine Maßnahmen der H5M

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Zutrittskontrolle:** Die Geschäftsräume in Marxzell sind abschließbar und nur einem eng begrenzten Personenkreis zugänglich. Server stehen dort nicht; die Plattform läuft in einem zertifizierten Rechenzentrum des Hosting-Anbieters in Deutschland.
- **Hosting-Sicherheit:** Die Plattform läuft auf einem dedizierten virtuellen Server mit einem Linux-Betriebssystem mit Langzeitunterstützung. Eine Firewall des Hosting-Anbieters lässt keine eingehenden Verbindungen zu; Datenbanken und interne Dienste sind nur innerhalb des Servers erreichbar.
- **Edge-Sicherheit:** Von außen ist die Plattform nur über einen verschlüsselten Tunnel eines Edge-Anbieters erreichbar, der die Anfragen über Sicherheitsregeln filtert und vor Überlastungsangriffen schützt. Die Verwaltungsoberfläche der Plattform erfordert eine Anmeldung über den eigenen Identitätsanbieter und lässt nur ausdrücklich zugelassene Konten zu; die Betriebszugänge (Bereitstellung, Fernwartung des Servers, Statusseite) sichert zusätzlich eine vorgeschaltete Anmeldung beim Edge-Anbieter.
- **Zugangskontrolle:**
 - Mehr-Faktor-Authentifizierung für die Konten der Auftragsverarbeiterin in Microsoft 365 (Bestätigung per Nummernabgleich oder mit Sicherheitsschlüssel) und für die administrativen Zugänge zu Hosting, Edge-Dienst, Code-Verwaltung und Bereitstellung.
 - Getrennte administrative Konten für die Verwaltung von Kundenumgebungen, ebenfalls mit Mehr-Faktor-Authentifizierung.
 - Passwörter: zentrale Verwaltung in einem Passwort-Tresor mit Ende-zu-Ende-Verschlüsselung; Mindestlänge 14 Zeichen, bei administrativen Konten 16 Zeichen, vom Passwort-Manager erzeugt, keine Mehrfachverwendung, keine Weitergabe per E-Mail oder Chat.
 - Administrativer Zugang zum Server von außen ausschließlich über den verschlüsselten Tunnel mit vorgeschalteter Anmeldung; der öffentliche SSH-Port des Servers ist geschlossen.
- **Zugriffskontrolle (Need-to-know):**
 - Zugriff auf die Daten der Verantwortlichen erhalten nur Personen, die ihn für ihre Aufgaben benötigen; die Verwaltungsoberfläche der Plattform ist nur für namentlich zugelassene Konten der Auftragsverarbeiterin freigeschaltet.
 - Links, über die Kunden einzelne Vorgänge bearbeiten (etwa eine Unterschrift), sind zufällig erzeugt, auf den Vorgang beschränkt und nur befristet gültig.

- Maschinelle Schnittstellen der Plattform für Betrieb und Notfall sind durch ein eigenes Zugangsgeheimnis geschützt; Funktionen, die Datenbestände zurücksetzen können, sind zusätzlich abgeschaltet und werden nur für einen Notfall freigeschaltet.
- **Endgeräte-Sicherheit:**
 - Die Endgeräte der Auftragsverarbeiterin werden zentral verwaltet, sind vollständig verschlüsselt und durch Bildschirmsperre geschützt; mobile Geräte lassen sich aus der Ferne löschen.
 - Endpoint-Schutz: verwaltete Lösungen für Endpoint-Schutz und Angriffserkennung auf den Endgeräten; Patch-Management und Monitoring über eine RMM-Plattform mit Betrieb und Hosting in Deutschland.
- **Datenträger:** Datenträger der Endgeräte sind vollständig verschlüsselt; vor ihrer Aussonderung werden sie sicher gelöscht oder zerstört.
- **Verschwiegenheit:** Alle Beschäftigten sind schriftlich auf die Vertraulichkeit verpflichtet; die Verpflichtungen sind dokumentiert.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Verschlüsselung bei der Übertragung:** Verbindungen zur Plattform sind mit TLS verschlüsselt; die Plattform weist Browser an, sie ausschließlich verschlüsselt aufzurufen (HSTS).
- **Verschlüsselung bei der Speicherung:**
 - Datensicherungen der Plattform werden vor dem Verlassen des Servers asymmetrisch verschlüsselt; der private Schlüssel liegt nicht auf der Plattform, sondern ausschließlich im Passwort-Tresor der Geschäftsführung.
 - Endgeräte der Auftragsverarbeiterin sind vollständig verschlüsselt.
- **Protokollierung:**
 - Anmeldungen an der Plattform, Änderungen über ihre Datenbank-Verwaltung, Aufrufe ihrer maschinellen Schnittstellen, Exporte und ausgewählte fachliche Vorgänge werden mit Nutzer, Aktion und Zeitpunkt in einem Protokoll festgehalten, das die Datenbank gegen nachträgliches Ändern und Löschen sperrt; für Microsoft 365 führt Microsoft zusätzlich ein eigenes Überwachungsprotokoll.
 - Jeder Sicherungslauf wird mit Prüfsummen, Ergebnis der Verifikation und Sperrstatus protokolliert.
- **Eingabe- und Änderungskontrolle:** Änderungen an der Plattform werden versioniert; der reguläre Weg in den Betrieb führt über automatische Prüfungen (Tests, Prüfung der Abhängigkeiten auf bekannte Schwachstellen, Suche nach Geheimnissen im Code). Vor jeder Änderung des Datenbankschemas wird automatisch gesichert; ohne erfolgreiche Sicherung unterbleibt die Änderung.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

■ Datensicherung der Plattform:

- Die Datenbanken der Plattform werden mindestens stündlich vollständig gesichert und verschlüsselt (siehe 2.).
- Die Sicherungen liegen bei zwei voneinander unabhängigen Speicheraanbietern (Anlage 2): die erste Sicherung jedes Tages bei beiden, die übrigen beim zweiten. Dort sind sie für ihre Aufbewahrungsfrist gegen Löschen und Ändern gesperrt; die Tagessicherungen werden 30 Tage, die übrigen zwei Tage aufbewahrt und danach automatisch gelöscht.
- Die auf der Plattform abgelegten Dateien werden täglich in den Speicher des zweiten Anbieters kopiert.
- Der Hosting-Anbieter sichert zusätzlich täglich ein Abbild des gesamten Servers und bewahrt es sieben Tage auf.

■ Datensicherung für Microsoft 365: Für Verantwortliche, die die Sicherung ihres Microsoft 365 gebucht haben, sichert ein spezialisierter Anbieter (Anlage 2) Postfächer, OneDrive, SharePoint und Teams getrennt von Microsoft in Rechenzentren in Deutschland.

■ Überwachung: Die Plattform wird laufend auf Erreichbarkeit, Sicherungen, Zertifikate und Ablauf von Zugangsdaten überwacht; Ausfälle meldet sie per E-Mail und Push-Nachricht. Der Edge-Anbieter schützt vor Überlastungsangriffen.

■ Notfallvorsorge: Ein schriftliches Notfallhandbuch beschreibt die Wiederherstellung der Plattform Schritt für Schritt.

4. Auftragskontrolle (Art. 32 Abs. 1 lit. b DSGVO i. V. m. Art. 28)

- Die Unterauftragsverarbeiter werden mit ihren Verträgen nach Art. 28 DSGVO, Übermittlungsgrundlagen und Prüfterminen in einem Lieferantenverzeichnis geführt.
- Weisungen, Meldungen und Nachweise gegenüber der Verantwortlichen laufen in Textform und werden dokumentiert.

5. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Nach jeder Sicherung prüft die Plattform automatisch, dass sich der Datenbestand in eine getrennte Datenbank einspielen lässt. Monatlich holt sie zusätzlich eine abgelegte Sicherung zurück und prüft sie auf Unversehrtheit.
- Die vollständige Wiederherstellung einer abgelegten Sicherung einschließlich Entschlüsselung wird mindestens einmal im Jahr geprobt und in der Plattform nachgewiesen.
- Für Verantwortliche mit gebuchter Microsoft-365-Sicherung lassen sich einzelne E-Mails, Dateien und Unterhaltungen bis hin zu ganzen Postfächern, OneDrive-Konten und SharePoint-Websites wiederherstellen.

- Endgeräte der Auftragsverarbeiterin lassen sich über die zentrale Geräteverwaltung neu einrichten.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Überprüfung der Maßnahmen mindestens jährlich und aus Anlass (§ 8 Abs. 2) im Rahmen des Informationssicherheits-Managementsystems mit Risiken, Maßnahmen, Lieferanten und Vorfällen.
- Die Plattform prüft täglich ihre Software-Abhängigkeiten auf bekannte Schwachstellen und gleicht die Versionen der eingesetzten Container und die verfügbaren Updates des Betriebssystems ab; Sicherheitsupdates des Betriebssystems spielt der Server automatisch ein.
- Datenpannen und Sicherheitsvorfälle werden nach einem festgelegten Ablauf mit Fristenkontrolle erfasst und ausgewertet.

7. Pseudonymisierung und Datenminimierung (Art. 32 Abs. 1 lit. a, Art. 5 DSGVO)

- Aufbewahrungsfristen sind je Datenart in einem Löschkonzept festgelegt; die Plattform setzt sie täglich automatisch durch und protokolliert jeden Lauf.
- Wo ein Vorgang als Nachweis erhalten bleibt, entfernt sie nach Ablauf der Frist die personenbezogenen Angaben, etwa IP-Adressen im Protokoll und E-Mail-Adressen im Versandprotokoll nach zwölf Monaten.
- Sicherheitsmeldungen von Endgeräten werden vor einer KI-Einschätzung um Benutzer-, Geräte- und Pfadangaben bereinigt.

Teil B: Besondere Maßnahmen für den Sicherheitscheck

1. **Nur Lesen:** Die Anwendung hat ausschließlich lesende Anwendungsrechte, dazu für die Anmeldung nur die delegierten Rechte `openid` und `profile`; der Abrufdienst stellt an den Tenant nur lesende Anfragen, auch innerhalb von Sammelabfragen.

2. **Richtiger Tenant und befugte Person:** Zustimmung bei Microsoft und Anmeldung der zustimmenden Person sind ein Schritt (OpenID Connect mit PKCE und Nonce); den Anmeldecode gibt Microsoft erst nach der Zustimmung aus. Das von Microsoft signierte ID-Token holt H5M mit diesem Code direkt bei Microsoft ab, prüft Empfänger und Nonce und übernimmt daraus nur die Kennungen von Tenant und Konto. H5M bindet die Bestellung erst danach an einen Tenant, und nur an den, den das ID-Token nennt; eine Rückleitung aus einem anderen als dem erwarteten Tenant oder ohne Anmeldung wird abgelehnt. Vor dem ersten Abruf prüft H5M, dass das Konto dort die Microsoft-Entra-Rolle „Globaler Administrator“ oder „Administrator für privilegierte Rollen“ hat, direkt oder über eine Gruppe; ein Konto, das es im Tenant nicht gibt, etwa bei einer Anmeldung nur über eine GDAP-Beziehung, genügt nicht. Sonst ruft H5M nichts weiter ab. Token nur für den gebundenen Tenant; die Tenant-Kennung wird im Token und in den Organisationsdaten gegengeprüft. Ist die Bestellung an einen Tenant gebunden, beim Folge-Check von Anfang an, wird eine Zustimmung aus einem anderen Tenant abgelehnt.
3. **Freigabe-Link:** Zufallstoken mit 256 Bit, gespeichert nur als SHA-256-Hash, gültig bis zum Ende der jeweiligen Freigabefrist (90 Tage nach der Bestellung oder nach dem Versand des Links zum Nachholen); ein neuer Link macht den bisherigen ungültig. Die Rückleitung von Microsoft gilt nur einmal, nur mit einem signierten Status, nur in dem Browser, in dem die Freigabe begonnen wurde, und nur innerhalb einer Stunde. Das bloße Aufrufen des Links ändert nichts.
4. **Zeitliche Grenze:** Abruf nur zwischen Zustimmung und Übermittlung, höchstens 14 Tage; danach technisch gesperrt.
5. **Datensparsamkeit:** nur benötigte Felder; aus der Anmeldung nur die Kennungen von Tenant und Konto; Anmeldemethoden nur als Art; Weiterleitungen nur als Zieldomain; Anmeldeprotokolle und genutzte Mailprotokolle nur als Anzahl; aus Gruppen nur die Kennungen der Mitgliedskonten; von App-Registrierungen nur Name und Ablaufdatum der Geheimnisse; je Prüfpunkt nur eine begrenzte Auswahl von Namen als Beleg.
6. **Zugriff bei H5M:** nur der Geschäftsführer, Anmeldung über den zentralen Identitätsdienst von H5M mit einem namentlich zugelassenen Konto. Keine Übergabe an KI-Sprachmodelle, kein Export außer dem Bericht an den Verantwortlichen.
7. **Übermittlung:** verschlüsselt, nur an die Bestelladresse; ohne Rückfrage nur, wenn sie in einer Domain des geprüften Tenants liegt oder bei Bestellung durch einen IT-Dienstleister die angegebene Domain des betreuten Unternehmens zum geprüften Tenant gehört, sonst erst nach Rückfrage; Download-Link 30 Tage gültig.
8. **Löschung:** automatisch nach § 8 durch die Aufbewahrungsautomatik mit Protokoll.

9. **Zugangsdaten der Anwendung:** nur im Passwort-Tresor und als geschützte Einstellung der Plattform. Ob Microsoft der Anwendung noch Zugang gewährt, prüft die Plattform täglich; bei Verdacht wird das Geheimnis sofort gelöscht, womit jeder weitere Abruf endet.
10. **Technische Protokolle:** ohne Inhalte von E-Mails, Dateien, Chats oder Kalendern; sie enthalten vor allem Kennungen wie die des Tenants und die Auftragsnummer sowie Fehlermeldungen von Microsoft und dienen nur dem Betrieb und der Fehlersuche.
11. **Werkzeuge der H5M:** Die Anbieter der Werkzeuge für Endpoint-Schutz, Fernwartung (RMM) und Passwortverwaltung aus Teil A erhalten im Rahmen des Sicherheitschecks keine Tenant-Daten; die Plattform hat zu ihnen keine Schnittstelle. Tenant-Daten liegen auf der Plattform bei Hetzner und verschlüsselt in den Datensicherungen bei Cloudflare R2 und IONOS; E-Mails zum Auftrag liegen bei Microsoft und Hornetsecurity. Auf seinen Endgeräten sieht der Geschäftsführer Befunde und Bericht nur im Browser an.