

FÜR GESCHÄFTSKUNDEN (B2B)

Ergänzende Bedingungen

für den H5M Sicherheitscheck für Microsoft 365

High5Manufaktur GmbH

Am Buchenhain 2, 76359 Marxzell · h5m.de

Fassung 1.0 · Stand: 29.09.2026

Vertragstext für Bestellungen über h5m.de, mit Leistungsbeschreibung als Anlage

Ergänzende Bedingungen

für den H5M Sicherheitscheck für Microsoft 365

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

§ 1 Geltung und Rangfolge

- (1) Diese Bedingungen gelten für Verträge über den „H5M Sicherheitscheck für Microsoft 365“ („Sicherheitscheck“) und die Durchsprache, die der Kunde mit der High5Manufaktur GmbH („H5M“) über die Website h5m.de schließt, für den Folge-Check (§ 2 Abs. 7) und die Durchsprache als Nachkauf (§ 8 Abs. 4) über die Bestellseiten der H5M unter app.h5m.rocks, deren Link H5M dem Kunden per E-Mail schickt.
- (2) Vertragsbestandteile sind: (a) die Bestellung mit Paket und Preis in der Fassung der Auftragsbestätigung, (b) diese Bedingungen mit der Leistungsbeschreibung (Anlage), (c) die Vereinbarung zur Auftragsverarbeitung für den Sicherheitscheck („AVV Sicherheitscheck“), (d) Teil A der Allgemeinen Geschäftsbedingungen der H5M („AGB“) in der bei der Bestellung gültigen Fassung.
- (3) Bei Widersprüchen gehen vor: Individualabreden, dann in datenschutzrechtlichen Fragen die AVV Sicherheitscheck, dann diese Bedingungen mit Anlage, dann Teil A der AGB. Die Teile B und D der AGB gelten nicht. Teil C der AGB gilt nur für die Durchsprache und nur, soweit diese Bedingungen nichts anderes regeln; § 19 AGB gilt nicht.
- (4) An die Stelle von § 2 Abs. 2 AGB (Vertragsschluss) tritt § 4, an die Stelle von § 3 Abs. 2 und 3 AGB (Fälligkeit, Lastschrift) tritt § 5. § 5 AGB (Laufzeit und Kündigung) gilt nicht; der Sicherheitscheck ist eine einmalige Leistung.
- (5) AVV im Sinne von § 7 AGB ist für diese Verträge die AVV Sicherheitscheck.

§ 2 Pakete und Leistungsumfang

- (1) H5M bietet an:
 1. „Sicherheitscheck“: eine automatisierte, ausschließlich lesende Prüfung ausgewählter Sicherheitseinstellungen des Microsoft-365-Tenants des Kunden und die Übermittlung des Ergebnisses als Sicherheitsbericht (PDF). Der Sicherheitscheck läuft automatisch; eine individuelle Einschätzung und eine Besprechung sind nicht enthalten. H5M kann einen Bericht vor der Übermittlung zur Qualitätssicherung durchsehen und offensichtliche Fehlbewertungen berichtigen; ein Anspruch darauf besteht nicht.
 2. „Sicherheitscheck mit Durchsprache“: die Leistung nach Nr. 1 und zusätzlich eine Durchsprache nach § 8.

3. „Durchsprache“ (Nachkauf): eine Durchsprache nach § 8 zu einem bereits gekauften Sicherheitscheck.

4. „Folge-Check“: ein weiterer Sicherheitscheck nach Nr. 1 für denselben Tenant zum halben Preis, nach Abs. 7.

Eine Bestellung des Sicherheitschecks umfasst einen Prüflauf für genau einen Microsoft-365-Tenant, bei Bestellung durch einen IT-Dienstleister den Tenant des bei der Bestellung genannten Unternehmens. Einzelheiten regelt die Leistungsbeschreibung.

- (2) Der Sicherheitsbericht bewertet nach dem Prüfkatalog der H5M die in der Leistungsbeschreibung genannten Einstellungen, soweit sie zum Zeitpunkt der Abfrage über die Schnittstellen von Microsoft mit den dort genannten Leserechten abrufbar sind, und die öffentlichen DNS-Einträge der Mail-Domains. Die verbundenen Apps und ihre Rechte listet er ohne Bewertung auf. Er ist eine Momentaufnahme dieses Zeitpunkts. H5M schuldet die sorgfältige Erstellung des Berichts nach der Leistungsbeschreibung. Sie schuldet weder die vollständige Erfassung aller Sicherheitsrisiken noch einen bestimmten Sicherheitszustand des Tenants und übernimmt keine Garantie.
- (3) Nicht geschuldet sind insbesondere: die Umsetzung von Empfehlungen und die Behebung von Fehlern; Änderungen im Tenant; Penetrationstests, Schwachstellenscans und Angriffssimulationen; die Prüfung von Endgeräten, Netzwerken, Servern und anderer Software; die Prüfung von Inhalten wie E-Mails, Dateien oder Chats; eine Überwachung über den Zeitpunkt der Abfrage hinaus; Rechts-, Datenschutz- oder Steuerberatung; Bescheinigungen oder Nachweise gegenüber Dritten wie Versicherern, Prüfern oder Behörden. Umsetzungsleistungen erbringt H5M nur aufgrund eines gesonderten Auftrags.
- (4) Welche Prüfpunkte sich automatisch bewerten lassen, hängt von Lizenzen und Einstellungen des Tenants ab. Kann ein Prüfpunkt deshalb oder aus anderen Gründen, die H5M nicht zu vertreten hat (etwa Änderungen der Schnittstellen durch Microsoft), nicht bewertet werden, weist der Bericht ihn als „nicht prüfbar“ aus. Das ist kein Mangel. Die Leistungsbeschreibung nennt außerdem Einstellungen, die der Sicherheitscheck grundsätzlich nicht automatisch prüft.
- (5) Den geschuldeten Prüfumfang bestimmt der Prüfkatalog, wie ihn die Leistungsbeschreibung in der bei der Bestellung gültigen Fassung beschreibt. Funktionen, Prüfpunkte und Darstellungsformen, die dort nicht genannt sind, sind nicht geschuldet. H5M darf den Prüfkatalog weiterentwickeln, insbesondere an Änderungen von Microsoft anpassen; für den einzelnen Vertrag gilt der bei der Bestellung beschriebene Umfang.
- (6) Der Sicherheitscheck ist für Tenants mit bis zu 1.000 Benutzerkonten ausgelegt. Hat ein Tenant mehr Konten, wertet der Bericht nur die ersten 1.000 von Microsoft gelieferten Konten und zusätzlich alle Konten mit einer

Administratorrolle in Microsoft Entra aus und weist darauf auf der ersten Seite hin. Prüfpunkte, die alle Konten betreffen, weist er dann als „nicht prüfbar“ aus; einen in den ausgewerteten Konten gefundenen Mangel nennt er mit dem Hinweis, dass weitere Konten betroffen sein können.

- (7) Hat H5M dem Kunden einen Sicherheitsbericht übermittelt, kann der Kunde für denselben Tenant einmal einen weiteren Sicherheitscheck zum halben Preis bestellen („Folge-Check“); maßgeblich ist der Preis des Sicherheitschecks am Tag der Bestellung des Folge-Checks. Bestellen kann der Kunde den Folge-Check ab der Übermittlung des Berichts, ohne Wartezeit, bis zu dem Tag, den H5M in der E-Mail mit dem Bericht nennt; dieses Bestellfenster ist mindestens sechs Monate lang. Der Folge-Check gilt nur für den Tenant des ersten Sicherheitschecks; eine Freigabe aus einem anderen Tenant lehnt H5M ab. Im Übrigen ist der Folge-Check ein Sicherheitscheck im Sinne dieser Bedingungen, auch für Freigabefrist, Verfall und Nachholen (§ 6 Abs. 8 und 9); es gelten diese Bedingungen und die AVV Sicherheitscheck in der bei seiner Bestellung gültigen Fassung. Zu einem Folge-Check gibt es keinen weiteren Folge-Check.

§ 3 Nur für Unternehmen mit Sitz in Deutschland

- (1) H5M schließt diese Verträge ausschließlich mit Unternehmern im Sinne von § 14 BGB mit Sitz in Deutschland, nicht mit Verbrauchern im Sinne von § 13 BGB. Juristische Personen des öffentlichen Rechts und öffentlich-rechtliche Sondervermögen bestellen bitte per E-Mail an info@h5m.de.
- (2) Mit der Bestellung bestätigt der Kunde, dass er in Ausübung seiner gewerblichen oder selbständigen beruflichen Tätigkeit handelt und seinen Sitz in Deutschland hat. Die bestellende Person bestätigt, dass sie den Kunden bei der Bestellung und beim Abschluss der AVV Sicherheitscheck vertreten darf.
- (3) Der Kunde gibt bei der Bestellung die Firma oder Bezeichnung seines Unternehmens und dessen Anschrift an. Hat H5M Zweifel, dass die Voraussetzungen nach Abs. 1 und 2 vorliegen, kann sie einen geeigneten Nachweis verlangen, etwa einen Registerauszug oder eine Gewerbeanmeldung, und die Bestellung bis zur Klärung ablehnen. Bestehen Anhaltspunkte, dass diese Voraussetzungen fehlen, kann H5M die Bestellung ablehnen oder, solange der Bericht nicht übermittelt ist, vom Vertrag zurücktreten. Gezahlte Beträge erstattet H5M bei einer Ablehnung oder einem Rücktritt vollständig.

§ 4 Bestellung und Vertragsschluss

- (1) Die Darstellung der Pakete auf der Website und den Bestellseiten ist kein bindendes Angebot.
- (2) Der Kunde wählt ein Paket, gibt die abgefragten Daten ein und bestätigt die Voraussetzungen nach § 3, die Geltung dieser Bedingungen und der AGB sowie

die Einbeziehung der AVV Sicherheitscheck. Vor dem Absenden zeigt die Bestellseite eine Übersicht; über „Angaben ändern“ kann der Kunde jede Eingabe berichtigen. Der Klick auf „Zahlungspflichtig bestellen“ führt zur Zahlseite des Zahlungsdienstleisters Stripe; dort bestätigt der Kunde diese Bedingungen noch einmal. Mit dem Abschluss des Bezahlvorgangs gibt der Kunde ein verbindliches Angebot auf Abschluss des Vertrags einschließlich der AVV Sicherheitscheck ab. Bis dahin kann er den Vorgang abbrechen.

- (3) H5M bestätigt den Eingang der Bestellung unverzüglich nach Abschluss des Bezahlvorgangs per E-Mail. Diese Eingangsbestätigung ist noch keine Annahme.
- (4) Der Vertrag kommt einschließlich der AVV Sicherheitscheck mit der Auftragsbestätigung per E-Mail zustande, die H5M nach Eingang der Zahlung versendet. Daten aus dem Tenant verarbeitet H5M erst nach der Freigabe durch den Kunden (§ 6). Bei sofort bestätigten Zahlarten fallen Eingangs- und Auftragsbestätigung in einer E-Mail zusammen. Geht die Zahlung nicht innerhalb von 14 Tagen nach der Bestellung ein, kommt kein Vertrag zustande.
- (5) H5M speichert den Vertragstext, also die Bestelldaten und die bei der Bestellung gültigen Fassungen dieser Bedingungen, der AVV Sicherheitscheck und der AGB. Der Kunde kann diese Texte vor der Bestellung abrufen und als PDF speichern und erhält sie mit der Auftragsbestätigung als PDF. Ein Kundenkonto gibt es nicht; frühere Fassungen sendet H5M auf Anfrage.
- (6) Vertragssprache ist Deutsch. H5M hat sich keinen Verhaltenskodizes unterworfen.

§ 5 Preise, Zahlung, Rechnung

- (1) Es gelten die Preise, die die Bestellseite angibt, netto zuzüglich der gesetzlichen Umsatzsteuer. Maßgeblich ist der Betrag, den die Zahlseite von Stripe vor dem Abschluss des Bezahlvorgangs nennt.
- (2) Der Preis ist bei der Bestellung im Voraus zu zahlen. Die Zahlung wickelt die Stripe Payments Europe, Limited, Dublin, Irland („Stripe“) über die von Stripe angebotenen Zahlarten ab. Ergänzend gelten die Bedingungen des gewählten Zahlungsmittels.
- (3) H5M beginnt mit der Leistung erst nach Eingang der Zahlung.
- (4) H5M stellt die Rechnung über den gesamten Preis nach Eingang der Zahlung aus, in der Regel am selben Tag, und übermittelt sie als elektronische Rechnung (ZUGFeRD, EN 16931) an die bei der Bestellung angegebene E-Mail-Adresse. Es ist eine Rechnung über eine Vorauszahlung für die noch zu erbringende Leistung; sie nennt den Tag der Zahlung. Nach der Leistung, bei einem Verfall (§ 6 Abs. 8, § 7 Abs. 4) und beim Nachholen (§ 6 Abs. 9) folgt keine weitere Rechnung. Umsatzsteuerrechtlich erforderliche Berichtigungen bleiben

unberührt, insbesondere wenn H5M den Preis ganz oder teilweise erstattet, nach einer Kündigung vor vollständiger Leistung (§ 10 Abs. 5) und wenn sich die umsatzsteuerliche Behandlung des gezahlten Betrags sonst nachträglich ändert; H5M stellt dann eine Rechnungskorrektur aus und berichtigt die Umsatzsteuer nach den gesetzlichen Vorschriften. Die Auftragsbestätigung und die Zahlungsbestätigung von Stripe sind keine Rechnungen.

- (5) Wird eine Zahlung zurückgebucht, etwa durch Rückbuchung einer Kartenzahlung, ohne dass der Kunde dazu berechtigt ist, bleibt der Anspruch auf den Preis bestehen. Hat der Kunde die Rückbuchung zu vertreten, ersetzt er die dadurch entstandenen Kosten.
- (6) Beauftragt der Kunde innerhalb von drei Monaten nach Übermittlung des Sicherheitsberichts eine laufende Betreuung nach Teil B der AGB, rechnet H5M einmalig den für den Sicherheitscheck gezahlten Nettopreis auf die ersten Entgelte dieser Betreuung an. Beim Paket „Sicherheitscheck mit Durchsprache“ ist das der Nettopreis, den der Sicherheitscheck allein am Tag der Bestellung gekostet hätte, nicht der Paketpreis. Eine Auszahlung ist ausgeschlossen.
- (7) Aktionscodes gelten nur für den Sicherheitscheck, nicht für das Paket „Sicherheitscheck mit Durchsprache“, die Durchsprache und den Folge-Check. Höhe, Gültigkeit und etwaige weitere Voraussetzungen nennt die jeweilige Aktion. Der Kunde kann einen Aktionscode nur bei der Bestellung einlösen, nicht nachträglich; je Bestellung gilt höchstens ein Aktionscode, und er lässt sich nicht mit anderen Nachlässen verbinden. Eine Auszahlung ist ausgeschlossen.

§ 6 Freigabe und Durchführung

- (1) Mit der Auftragsbestätigung erhält der Kunde einen Freigabe-Link. Er gilt bis zum Ende der Freigabefrist nach Abs. 8 und nur für diese Bestellung. Mit jeder Erinnerung nach Abs. 8, mit einer erneuten Anforderung nach Abs. 5 und auf Anfrage erzeugt H5M innerhalb dieser Frist einen neuen Link; der bisherige wird damit ungültig.
- (2) Über den Link meldet sich eine Person, die im zu prüfenden Tenant die Microsoft-Entra-Rolle „Globaler Administrator“ oder „Administrator für privilegierte Rollen“ hat („Freigaberolle“), bei Microsoft an und stimmt dabei der Anwendung „H5M Sicherheitsbericht“ zu; Anmeldung und Zustimmung sind ein Schritt. H5M bindet die Bestellung erst an einen Tenant, wenn Microsoft die Zustimmung bestätigt hat, und nur an den Tenant, in dem die Person angemeldet ist und zugestimmt hat. Vor dem ersten Abruf prüft H5M, dass das angemeldete Konto in diesem Tenant eine Freigaberolle hat; fehlt sie, gilt die Freigabe als nicht erteilt, und H5M ruft keine weiteren Daten ab. Der Kunde stellt sicher, dass eine befugte Person seines Unternehmens oder seines beauftragten IT-Dienstleisters zustimmt; sie braucht ein eigenes Konto im

Tenant, auch als Gast. Eine Freigaberolle nur über eine GDAP-Beziehung genügt nicht. Ist die Bestellung an einen Tenant gebunden, nimmt H5M für diese Bestellung keine Zustimmung aus einem anderen Tenant mehr an. Aus einem Tenant, an den die Bestellung nicht gebunden ist, ruft H5M nichts ab; eine dort erteilte Zustimmung kann der Kunde wie in Abs. 5 beschrieben entfernen.

- (3) Die Anwendung erhält zum Lesen des Tenants ausschließlich die in der Leistungsbeschreibung genannten Leserechte, für die Anmeldung nach Abs. 2 zusätzlich die Berechtigungen „openid“ und „profile“. Sie kann im Tenant nichts ändern und liest weder Inhalte von E-Mails, Dateien, Chats oder Kalendern noch Kennwörter. Der Kunde gestattet ausdrücklich, dass die Anwendung Postfacheinstellungen und Posteingangsregeln im Umfang der Leistungsbeschreibung liest.
- (4) H5M ruft den Tenant für eine Bestellung nur zwischen der Zustimmung und der Übermittlung des Berichts ab, höchstens bis 14 Tage nach der Zustimmung. Erneut abgefragt wird in dieser Zeit nur, wenn die erste Abfrage technisch gescheitert ist. Danach ruft H5M den Tenant für diese Bestellung nur noch ab, wenn der Kunde die Freigabe erneut erteilt, nach Abs. 5 oder zur Nacherfüllung (§ 10 Abs. 3); für die neue Zustimmung gelten die Sätze 1 und 2 entsprechend.
- (5) Der Kunde kann die Freigabe jederzeit selbst entfernen: Im Microsoft Entra Admin Center (entra.microsoft.com) unter „Unternehmensanwendungen“ die Anwendung „H5M Sicherheitsbericht“ öffnen, „Eigenschaften“ wählen und „Löschen“. H5M empfiehlt, die Anwendung nach Erhalt des Berichts zu entfernen. Entfernt der Kunde die Freigabe, bevor H5M den Tenant abgefragt hat, oder verweigert Microsoft den Zugriff aus einem anderen Grund dauerhaft, etwa weil die Zustimmung widerrufen wurde oder eine Berechtigung fehlt, fordert H5M die Freigabe per E-Mail an die Bestelladresse mit einem neuen Freigabe-Link erneut an, solange die Freigabefrist läuft. Der Kunde muss die Freigabe dann innerhalb der Freigabefrist erneut erteilen; sonst gilt Abs. 8.
- (6) Der Kunde sorgt dafür, dass der Sicherheitscheck in seinem Unternehmen zulässig durchgeführt werden kann. Er informiert insbesondere, soweit erforderlich, seine Beschäftigten und wahrt etwaige Beteiligungsrechte eines Betriebsrats.
- (7) Bestellt der Kunde als IT-Dienstleister für den Tenant eines von ihm betreuten Unternehmens, gibt er dieses Unternehmen und dessen Domain bei der Bestellung an. Das ist nur zulässig, wenn der Kunde für diese Verarbeitung Auftragsverarbeiter des betreuten Unternehmens ist; bestellt er nur als dessen Vertreter, ist das betreute Unternehmen selbst als Kunde anzugeben. Der Kunde sichert zu, dass das betreute Unternehmen ihn mit der Betreuung seines Microsoft 365 beauftragt und genehmigt hat, dass H5M als weiterer Auftragsverarbeiter nach Art. 28 Abs. 2 DSGVO eingesetzt wird. Verletzt der Kunde diese Zusicherung schuldhaft, stellt er H5M von berechtigten

Ansprüchen des betreuten Unternehmens oder Dritter frei, soweit diese auf der Pflichtverletzung beruhen; eine von H5M zu vertretende Mitverursachung bleibt unberührt. H5M informiert den Kunden unverzüglich über geltend gemachte Ansprüche und gibt ihm Gelegenheit, an der Abwehr mitzuwirken. Im Übrigen gilt § 11 der AVV Sicherheitscheck.

- (8) Der Kunde sorgt dafür, dass die Freigabe nach Abs. 2 innerhalb von 90 Tagen nach der Bestellung erteilt wird (Freigabefrist); das Fristende nennt die Auftragsbestätigung mit Datum. H5M erinnert 14 und 76 Tage nach der Bestellung per E-Mail an die Bestelladresse an die ausstehende Freigabe. Liegt bis zum Fristende keine Freigabe vor, erlischt der Anspruch des Kunden auf Durchführung des Sicherheitschecks, beim Paket „Sicherheitscheck mit Durchsprache“ auch auf die Durchsprache. Der gezahlte Preis wird nicht allein wegen des Fristablaufs erstattet. Dem Kunden bleibt der Nachweis vorbehalten, dass H5M wegen der unterbliebenen Freigabe kein oder nur ein geringerer Anspruch auf Vergütung, Entschädigung oder Schadensersatz zusteht; einen danach nicht geschuldeten Betrag erstattet H5M. Konnte die Freigabe aus Gründen nicht erteilt werden, die H5M zu vertreten hat, oder weil Microsoft die Anwendung sperrt oder die Zustimmung technisch nicht zulässt, gilt § 10 Abs. 6 entsprechend; Einstellungen im Tenant des Kunden gehören nicht dazu. Das Fristende gilt auch, wenn eine Erinnerung den Kunden nicht erreicht. Das einmalige Nachholen nach Abs. 9 bleibt unberührt.
- (9) Ist der Anspruch nach Abs. 8 erloschen, teilt H5M das dem Kunden per E-Mail an die Bestelladresse mit. Der Kunde kann den Sicherheitscheck dann einmal ohne erneute Zahlung nachholen. Dazu fordert er innerhalb von zwölf Monaten nach dem Ende der Freigabefrist über den Link in der Mitteilung zum Verfall oder in Textform einen neuen Freigabe-Link an. Mit dem Versand dieses Links beginnt eine neue Freigabefrist von 90 Tagen; im Übrigen gelten Abs. 1 bis 8 entsprechend, beim Paket „Sicherheitscheck mit Durchsprache“ für das ganze Paket einschließlich der Durchsprache. Es gelten die Bedingungen und der Preis der ursprünglichen Bestellung. Verfällt der Anspruch erneut, ist er endgültig erloschen; ein weiteres Nachholen gibt es nicht.

§ 7 Leistungszeit und Übermittlung

- (1) H5M übermittelt den Sicherheitsbericht in der Regel innerhalb von 24 Stunden, spätestens fünf Werktage nach der Zustimmung. Werktage sind Montag bis Freitag außer den gesetzlichen Feiertagen in Baden-Württemberg.
- (2) Störungen oder Drosselungen der Microsoft-Dienste und andere Umstände, die H5M nicht zu vertreten hat, verlängern die Frist angemessen. Einen Anspruch auf ständige Verfügbarkeit der Bestellseite oder der Microsoft-Schnittstellen hat der Kunde nicht.

- (3) H5M übermittelt den Bericht per E-Mail an die bei der Bestellung angegebene Adresse als Link zum Herunterladen, der 30 Tage gilt. Solange H5M die Befunde nach der AVV Sicherheitscheck aufbewahrt, stellt sie auf Anfrage einen neuen Link bereit; der Bericht beruht dann auf denselben Befunden. Der Kunde speichert den Bericht selbst.
- (4) Ohne Rückfrage übermittelt H5M den Bericht nur, wenn (a) die bei der Bestellung angegebene E-Mail-Adresse in einer Domain des geprüften Tenants liegt oder (b) bei einer Bestellung als IT-Dienstleister nach § 6 Abs. 7 die angegebene Domain des betreuten Unternehmens zu den Domains des geprüften Tenants gehört. Sonst übermittelt H5M den Bericht erst nach Rückfrage beim Kunden; bis zu seiner Antwort läuft die Frist nach Abs. 1 nicht. Der Kunde bestätigt die Rückfrage über den Link darin oder auf anderem Weg gegenüber H5M. Bestätigt er sie nicht innerhalb von 90 Tagen nach ihrem Versand, ist H5M nicht mehr zur Übermittlung verpflichtet, und der Anspruch auf Übermittlung erlischt. Die Auswertung ist zu diesem Zeitpunkt abgeschlossen; nur die Übermittlung des Berichts scheitert an der fehlenden Bestätigung. H5M behält deshalb den Anspruch auf die Vergütung für die erbrachten Leistungen und rechnet an, was sie durch die unterbliebene Übermittlung erspart. Beim Paket „Sicherheitscheck mit Durchsprache“ erlischt dann auch der Anspruch auf die Durchsprache, die den Bericht voraussetzt; H5M erstattet dafür den Unterschied zwischen dem Preis des Pakets und dem Preis, den der Sicherheitscheck allein am Tag der Bestellung gekostet hätte, jeweils einschließlich Umsatzsteuer.

§ 8 Durchsprache

- (1) Die Durchsprache ist eine Besprechung des Sicherheitsberichts per Microsoft Teams oder Telefon von 45 Minuten. Sie umfasst die Erläuterung der Befunde und des Maßnahmenplans, die Priorisierung, Antworten auf Fragen des Kunden und auf Wunsch einen gemeinsamen Blick auf die nicht automatisch geprüften Einstellungen über eine Bildschirmfreigabe des Kunden. Der Kunde achtet dabei darauf, nur die für die Durchsprache nötigen Einstellungen zu zeigen und keine Inhalte und keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) einzublenden. H5M meldet sich nicht im Tenant an und ändert nichts. Umsetzung und Fehlerbehebung sind nicht enthalten. H5M zeichnet die Durchsprache nicht auf.
- (2) Den Termin bucht der Kunde über die in der Auftragsbestätigung und in der E-Mail mit dem Bericht genannte Terminbuchung oder per E-Mail. Die Durchsprache findet innerhalb von drei Monaten nach Übermittlung des Berichts statt; danach verfällt der Anspruch auf die Durchsprache. H5M erinnert spätestens zwei Wochen vor Ablauf per E-Mail an die Bestelladresse.

- (3) Der Kunde kann einen Termin bis 24 Stunden vorher kostenfrei absagen oder verlegen. Nimmt er einen Termin ohne rechtzeitige Absage nicht wahr oder bucht er innerhalb der Frist nach Abs. 2 keinen Termin, behält H5M den Anspruch auf die Vergütung (§ 615 Satz 1 BGB). Sie muss sich anrechnen lassen, was sie infolge des Unterbleibens der Durchsprache erspart oder durch anderweitige Verwendung ihrer Dienste erwirbt oder zu erwerben böswillig unterlässt (§ 615 Satz 2 BGB).
- (4) Die Durchsprache als Nachkauf kann nur bestellen, wer einen Sicherheitscheck gekauft hat, und nur innerhalb von drei Monaten nach Übermittlung des Berichts, solange in dieser Zeit noch ein Termin frei ist. Für Bestellung, Vertragsschluss und Zahlung gelten die §§ 3 bis 5 entsprechend. Die bei der Bestellung des Sicherheitschecks geschlossene AVV Sicherheitscheck gilt fort.

§ 9 Nutzung und Vertraulichkeit des Berichts

- (1) Der Bericht ist vertraulich und für den Kunden bestimmt. Der Kunde erhält ein einfaches, zeitlich unbeschränktes, nicht übertragbares Recht, ihn für eigene Zwecke zu nutzen und an Berater, Dienstleister, Versicherer und Prüfer weiterzugeben, die er zur Vertraulichkeit verpflichtet. Bestellt der Kunde als IT-Dienstleister (§ 6 Abs. 7), darf er den Bericht dem betreuten Unternehmen überlassen; dieses darf ihn im selben Umfang nutzen. Eine Veröffentlichung des Berichts oder seiner Ergebnisse, auch auszugsweise oder zu Werbezwecken, bedarf der vorherigen Zustimmung von H5M in Textform.
- (2) H5M nennt den Kunden nicht als Referenz und veröffentlicht keine Ergebnisse aus dem Sicherheitscheck.
- (3) Aufbau, Prüfkatalog und Texte des Berichts bleiben geistiges Eigentum von H5M.

§ 10 Abnahme, Mängel, Beendigung

- (1) Die Erstellung des Sicherheitsberichts ist eine Werkleistung (§§ 631 ff. BGB), die Durchsprache eine Dienstleistung (§§ 611 ff. BGB).
- (2) Ein Mangel liegt insbesondere vor, wenn der Bericht die zum Zeitpunkt der Abfrage gelesenen Einstellungen unrichtig wiedergibt oder von der Leistungsbeschreibung abweicht. Kein Mangel sind: als „nicht prüfbar“ ausgewiesene Punkte, soweit § 2 Abs. 4 oder 6 dies vorsieht; Änderungen im Tenant nach der Abfrage; Einstellungen, die der Sicherheitscheck nach der Leistungsbeschreibung nicht prüft; die Bewertung einer Einstellung nach dem Prüfkatalog, auch wenn andere Prüfverfahren sie anders bewerten würden.
- (3) Mit der Übermittlung setzt H5M eine Frist von 14 Tagen zur Abnahme (§ 640 Abs. 2 BGB). H5M beseitigt Mängel nach ihrer Wahl durch Berichtigung oder neue Erstellung; dafür kann eine erneute Freigabe nötig sein. Schlägt die Nacherfüllung fehl, gelten die gesetzlichen Rechte.

- (4) Ansprüche wegen Mängeln verjähren in zwölf Monaten ab Abnahme. Das gilt nicht für Ansprüche auf Schadensersatz in den Fällen des § 6 Abs. 1 und 2 AGB und nicht, soweit das Gesetz längere Fristen zwingend vorschreibt; dafür gelten die gesetzlichen Fristen. Für Schadensersatz gilt im Übrigen § 6 AGB.
- (5) Der Kunde kann den Vertrag bis zur Übermittlung des Berichts jederzeit in Textform kündigen (§ 648 BGB); beim Paket „Sicherheitscheck mit Durchsprache“ gilt die Kündigung für das ganze Paket einschließlich der Durchsprache. H5M rechnet die vereinbarte Vergütung dann nach § 648 Satz 2 und 3 BGB ab und berücksichtigt insbesondere, was sie infolge der Kündigung an Aufwendungen erspart oder durch anderweitige Verwendung ihrer Arbeitskraft erwirbt oder zu erwerben böswillig unterlässt. Sie legt die Berechnung auf Verlangen nachvollziehbar dar; dem Kunden bleibt der Nachweis höherer anzurechnender Beträge vorbehalten. Eine Durchsprache, die noch nicht stattgefunden hat, kann der Kunde auch nach Übermittlung des Berichts und als Nachkauf in Textform kündigen; für die Vergütung gelten die Sätze 2 und 3 entsprechend. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.
- (6) Kann H5M den Bericht aus Gründen, die sie nicht zu vertreten hat, nicht erstellen, etwa weil Microsoft den Zugriff der Anwendung sperrt oder Schnittstellen einstellt, kann jede Partei vom Vertrag zurücktreten. H5M erstattet den gezahlten Preis dann vollständig.
- (7) Ob und wie Empfehlungen umgesetzt werden, entscheidet der Kunde. H5M empfiehlt, Änderungen vorher auf ihre Auswirkungen im eigenen Betrieb zu prüfen.

§ 11 Datenschutz

- (1) Die aus dem Tenant gelesenen personenbezogenen Daten verarbeitet H5M ausschließlich als Auftragsverarbeiter nach der AVV Sicherheitscheck. Für eigene Zwecke nutzt sie diese Daten nicht, insbesondere nicht für Werbung, Auswertungen oder Statistiken.
- (2) Daten aus Bestellung, Zahlung und Vertragsabwicklung einschließlich des Nachweises der Freigabe (§ 6 Abs. 2) verarbeitet H5M als Verantwortliche nach ihrer Datenschutzerklärung (h5m.de/datenschutz).

§ 12 Fassungen, Schlussbestimmungen

- (1) Für jeden Vertrag gilt die bei der Bestellung gültige Fassung dieser Bedingungen. Spätere Fassungen gelten nur für spätere Bestellungen.
- (2) Im Übrigen gilt § 10 AGB.

Hinweis:

Microsoft 365 und Microsoft Entra sind Marken der Microsoft-Unternehmensgruppe. H5M ist ein unabhängiger Anbieter; der Sicherheitscheck wird von Microsoft weder angeboten noch geprüft oder unterstützt.

Anlage: Leistungsbeschreibung

1. Pakete (Preise laut Bestellseite zum Zeitpunkt der Bestellung)

- **Sicherheitscheck:** automatische Prüfung eines Microsoft-365-Tenants und Bericht als PDF, ohne persönliche Einschätzung und Besprechung; H5M kann den Bericht vor der Übermittlung zur Qualitätssicherung durchsehen (§ 2 Abs. 1 der Bedingungen).
- **Sicherheitscheck mit Durchsprache:** zusätzlich eine Durchsprache von 45 Minuten.
- **Durchsprache (Nachkauf):** 45 Minuten, nur nach Kauf eines Sicherheitschecks, bestellbar bis drei Monate nach Übermittlung des Berichts, solange in dieser Zeit noch ein Termin frei ist.
- **Folge-Check:** ein weiterer Sicherheitscheck für denselben Tenant zum halben Preis, einmal bestellbar ab der Übermittlung des Berichts bis zu dem Tag, den die E-Mail mit dem Bericht nennt, mindestens sechs Monate lang (§ 2 Abs. 7 der Bedingungen).

Jeder Sicherheitscheck, auch im Paket und als Folge-Check, setzt voraus, dass der Kunde den Zugriff innerhalb von 90 Tagen nach der Bestellung freigibt. Sonst erlischt der Anspruch auf Durchführung; eine Erstattung gibt es dann grundsätzlich nicht (§ 6 Abs. 8 der Bedingungen). Der Kunde kann den Check aber einmal innerhalb von zwölf Monaten nach dem Verfall ohne erneute Zahlung nachholen (Nr. 3).

2. Voraussetzungen

- ein Microsoft-365-Tenant eines Unternehmens (Microsoft Entra ID);
- eine Person mit eigenem Konto im Tenant (auch als Gast), die dort die Microsoft-Entra-Rolle „Globaler Administrator“ oder „Administrator für privilegierte Rollen“ hat (Freigaberolle) und innerhalb der Freigabefrist bei Microsoft zustimmt und sich anmeldet; eine Freigaberolle nur über eine GDAP-Beziehung genügt nicht;
- bis zu 1.000 Benutzerkonten.

Manche Angaben, etwa die letzte Anmeldung je Konto, liefert Microsoft nur mit Microsoft Entra ID P1, das zum Beispiel in Business Premium enthalten ist. Ohne P1 nutzt der Sicherheitscheck den Nutzungsbericht der letzten 90 Tage oder weist den Punkt als nicht prüfbar aus.

3. Ablauf

1. Bestellung und Zahlung; die Rechnung über den gesamten Preis kommt direkt danach per E-Mail.
2. Auftragsbestätigung mit Freigabe-Link. Die Freigabe muss innerhalb von 90 Tagen nach der Bestellung erfolgen (Fristende mit Datum in der Auftragsbestätigung); H5M erinnert nach 14 und nach 76 Tagen.

3. Anmeldung und Zustimmung bei Microsoft in einem Schritt durch eine Person mit Freigaberolle (Nr. 2); vor dem ersten Lesen prüft H5M die Freigaberolle.
4. Automatische, nur lesende Abfrage und Auswertung; vor der Übermittlung gegebenenfalls eine Durchsicht zur Qualitätssicherung (§ 2 Abs. 1 der Bedingungen).
5. Bericht per E-Mail als Link zum Herunterladen (30 Tage gültig), in der Regel innerhalb von 24 Stunden, spätestens fünf Werktage nach der Zustimmung; passt weder die bei der Bestellung angegebene Adresse noch, bei Bestellung als IT-Dienstleister, die angegebene Domain des betreuten Unternehmens zum geprüften Tenant, erst nach Rückfrage (§ 7 Abs. 4 der Bedingungen).
6. Der Kunde entfernt die Anwendung (empfohlen).
7. Falls gebucht: Durchsprache innerhalb von drei Monaten nach dem Bericht.

Ohne Freigabe innerhalb der Frist erlischt der Anspruch auf Durchführung, beim Paket insgesamt; eine Erstattung gibt es dann grundsätzlich nicht (§ 6 Abs. 8 der Bedingungen). Der Kunde kann den Check einmal innerhalb von zwölf Monaten nach dem Verfall ohne erneute Zahlung nachholen; dann beginnt eine neue Freigabefrist von 90 Tagen (§ 6 Abs. 9 der Bedingungen). Verweigert Microsoft den Zugriff nach der Zustimmung dauerhaft, fordert H5M die Freigabe erneut an (§ 6 Abs. 5 der Bedingungen). Bleibt eine Rückfrage vor der Übermittlung 90 Tage unbestätigt, erlischt der Anspruch auf die Übermittlung; beim Paket erstattet H5M dann den Unterschied zum Preis des Sicherheitschecks am Tag der Bestellung (§ 7 Abs. 4 der Bedingungen). Kündigt der Kunde vor Übermittlung des Berichts, rechnet H5M nach § 648 BGB ab (§ 10 Abs. 5 der Bedingungen).

4. Leserechte der Anwendung „H5M Sicherheitsbericht“ (Microsoft Graph, Anwendungsberechtigungen, alle nur lesend)

- **Directory.Read.All:** Benutzer, Gruppen, Rollen, Domains, Lizenzen, verbundene Apps, Gruppeneinstellungen und Ablaufdaten der App-Registrierungen (keine Geheimnisse)
- **Policy.Read.All:** Sicherheitsstandards, Richtlinien für bedingten Zugriff, erlaubte Anmeldemethoden, die ältere Einstellung „MFA pro Benutzer“, Einstellungen zu Gästen und Apps
- **UserAuthenticationMethod.Read.All:** welche Anmeldemethoden eingerichtet sind (keine Geheimnisse)
- **AuditLog.Read.All:** letzte Anmeldung je Konto, Anmeldungen über veraltete Verfahren und Registrierungsstand der Anmeldemethoden
- **MailboxSettings.Read:** Postfachtyp und Posteingangsregeln, keine E-Mails
- **SecurityEvents.Read.All:** Microsoft Secure Score und seine Einzelmaßnahmen
- **SharePointTenantSettings.Read.All:** Freigabe-Einstellungen und automatische Abmeldung von SharePoint und OneDrive

- **Reports.Read.All:** Nutzungsberichte der letzten 90 Tage (ungenutzte Konten, genutzte Mailprotokolle)

Dazu kommen öffentliche Angaben zu den Mail-Domains: die DNS-Einträge MX, SPF, DKIM, DMARC, MTA-STS und TLS-RPT, ob die Domain mit DNSSEC signiert ist, sowie die öffentliche MTA-STS-Regeldatei, die H5M wie jeder sendende Mailserver abrufen.

Für die Anmeldung bei der Freigabe hat die Anwendung außerdem die delegierten Berechtigungen openid und profile (Anmeldung und Basisprofil der zustimmenden Person); Microsoft zeigt sie im Zustimmungsdialog mit an. H5M übernimmt daraus nur die Kennung des Tenants und des Kontos und prüft mit Directory.Read.All dessen Freigaberolle (Nr. 2).

5. Was die Anwendung nicht tut

- keine Änderungen im Tenant;
- keine Inhalte von E-Mails, Dateien, Chats oder Kalendern;
- keine Kennwörter oder Geheimnisse.

Von Anmeldemethoden übernimmt der Sicherheitscheck nur die Art, nicht Telefonnummern oder Gerätenamen; von Weiterleitungsregeln nur das Postfach, den Namen der Regel, ob sie eingeschaltet ist, und die Domain des Ziels, nicht die vollständige Adresse; von App-Registrierungen nur den Namen und das Ablaufdatum der Geheimnisse und Zertifikate; von den Kennwortregeln nur, ob ein Konto davon ausgenommen ist.

6. Prüfumfang

Der Sicherheitscheck prüft diese Punkte (Prüfkatalog nach § 2 Abs. 5 der Bedingungen):

- **Anmeldung und Konten:** zweite Anmeldestufe für alle vorgeschrieben; bei allen Mitarbeitenden eingerichtet; unsichere Anmeldemethoden abgeschaltet; Administratoren mit der zweiten Stufe geschützt; Notfallkonto eingerichtet und geschützt; zwei bis vier globale Administratoren; Administratoren ohne Alltagskonto; Administratorrollen nur für eigene, reine Cloud-Konten; keine seit Monaten ungenutzten aktiven Konten; Gastzugänge überschaubar und Einladungen geregelt; kein erzwungener Kennwortablauf; kein Konto von den Kennwortregeln ausgenommen.
- **E-Mail:** keine Posteingangsregeln, die Mails nach außen weiterleiten; automatische Weiterleitung nach außen gesperrt; geteilte Postfächer ohne direkte Anmeldung; kein zweiter Weg am Mailfilter vorbei; SPF; DKIM; DMARC; Schutzrichtlinien gegen Phishing und Schadsoftware; keine Nutzung älterer Mailprotokolle (POP, IMAP, SMTP); verschlüsselte Zustellung (MTA-STS und TLS-RPT); signierte DNS-Einträge (DNSSEC).

- **Apps und Freigaben:** keine Zustimmung von Mitarbeitenden zu fremden Apps; Registrierung eigener Apps nur durch Administratoren; Gäste sehen nur, was sie sehen sollen; keine Freigabe-Links, die ohne Anmeldung funktionieren; automatische Abmeldung bei Inaktivität im Browser; Sperre veralteter Anmeldeverfahren ohne zweite Stufe; kein unbemerkter Ablauf der Zugänge eigener App-Registrierungen.
- **Verwaltung:** technische Kontaktadresse bei Microsoft; nicht vergebene Lizenzen; keine halb eingerichteten Domains; Sicherung der Daten in Microsoft 365; Auditprotokoll eingeschaltet; keine Selbstanmeldung an Diensten und keine eigenen Tenants durch Mitarbeitende.

Einzelne Punkte ermittelt der Sicherheitscheck aus den Maßnahmen des Microsoft Secure Score. Ohne Bewertung listet der Bericht außerdem die verbundenen Apps mit weitreichenden Rechten auf, damit der Kunde sie durchgehen kann; die Liste zählt nicht in das Ergebnis.

7. Nicht automatisch geprüft (im Bericht mit einer kurzen Anleitung zum Selbstprüfen)

Weiterleitung direkt am Postfach; einfacher SMTP-Versand (SMTP AUTH); POP und IMAP je Postfach; Kennzeichnung externer Absender; Teams: Gäste und fremde Organisationen; Voreinstellung und Ablauf von Freigabe-Links; Käufe und Testabos durch Mitarbeitende.

Ebenso nennt der Bericht mit Anleitung die Punkte, die im jeweiligen Tenant nicht automatisch prüfbar waren.

8. Bewertung

- **Stände:** In Ordnung, Teilweise, Handlungsbedarf, Nicht zutreffend, Nicht prüfbar; die Liste der verbundenen Apps steht ohne Wertung als „Zur Kenntnis“ im Bericht.
- **Gewichtung:** kritisch dreifach, wichtig doppelt, empfohlen einfach; „Teilweise“ zählt halb.
- Nicht zutreffende und nicht prüfbare Punkte sowie die Liste „Zur Kenntnis“ zählen nicht.
- Ergebnis ist der Anteil der erreichten an den möglichen Punkten als Wert von 0 bis 100 mit einer Einstufung in Worten. Zusätzlich nennt der Bericht den Microsoft Secure Score, soweit Microsoft ihn liefert; das ist Microsofts eigene Bewertung.

9. Inhalt des Berichts

Der Bericht nennt Name, Kennung und Domains des geprüften Tenants, wie Microsoft sie meldet. Er enthält: Ergebnis auf einen Blick, Maßnahmenplan nach Dringlichkeit mit einem Hinweis auf die Liste der verbundenen Apps, alle Prüfpunkte mit Befund, Begründung und Empfehlung, die Liste der verbundenen Apps mit ihren Rechten ohne Wertung, die nicht automatisch geprüften und die im Tenant nicht prüfbareren Einstellungen mit einer kurzen Anleitung zum Selbstprüfen, Methode und Datenschutz, Anleitung zum Entfernen der Anwendung. Als Beleg nennt er je Prüfpunkt nur eine begrenzte Auswahl betroffener Konten; lange Listen kürzt er.

10. Datenschutz

Nach der AVV Sicherheitscheck. Die Rohdaten werden mit Übermittlung des Berichts gelöscht, spätestens 30 Tage nach dem Abruf, die Befunde 90 Tage nach der Übermittlung, bei gebuchter Durchsprache 30 Tage nach der Durchsprache, spätestens sechs Monate nach der Übermittlung. Wird kein Bericht übermittelt, werden die Befunde gelöscht, sobald das feststeht, spätestens am Tag nach Ablauf von 90 Tagen nach dem Abruf, bei einer Rückfrage am Tag nach Ablauf von 90 Tagen nach deren Versand (§ 8 der AVV Sicherheitscheck).