



HanseSecure

CHOOSE THE INTRUDER!

**AGB
ALLGEMEINE
GESCHÄFTSBEDINGUNGEN**



1 INHALTSVERZEICHNIS

1	Inhaltsverzeichnis.....	2
2	Dokumenteninformation	3
3	Geltungsbereich	3
4	Begriffsbestimmungen.....	4
5	Penetrationstests.....	4
6	Phishingtest.....	9
7	Einwilligung bzgl. Straftatbeständen (Hacker-Paragrafen).....	11
8	Vertragsschluss und Leistungsänderungen.....	12
9	Vergütung und Zahlungsbedingungen.....	12
10	Vertragslaufzeit und Kündigung	13
11	Haftung	14
12	Datenschutzhinweise	15
13	Geheimhaltungs- und Referenzklausel.....	16
14	Abwerbung von Mitarbeitern.....	16
15	Nutzungsrechte und geistiges Eigentum	17
16	Keine Erfolgsgarantie	17
17	Schlussbestimmungen	17

Angebote der Firma HanseSecure GmbH (Auftragnehmer), sowie jegliche bereitgestellte Dokumente sind ausschließlich für den unmittelbaren Auftraggeber bestimmt und müssen vertraulich behandelt werden. Die Weitergabe und Vervielfältigung aller Unterlagen, sowie die Verwertung und Mitteilung des Inhaltes an Dritte ist nicht gestattet. Zuwiderhandlungen verpflichten zum Schadensersatz. Aufgrund der besseren Lesbarkeit wird im Text das generische Maskulinum verwendet. Die in diesem Konzept

*** verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter. = ***

2 DOKUMENTENINFORMATION

Version	5
Klassifizierung	Offen

3 GELTUNGSBEREICH

3.1

Diese Allgemeinen Geschäftsbedingungen (fortan „AGB“ genannt) gelten in der zum Zeitpunkt eines Vertragsschlusses gültigen Fassung für alle Verträge über die Leistungen von HanseSecure GmbH (Geschäftsführung: Florian Hansemann, Nicole Maronn-Hansemann), Thalkirchner Str. 7, 80337 München, Deutschland, (fortan „Dienstleister“ genannt), die mit seinem Kunden („Kunde“) geschlossen werden. Der Dienstleister ist ein White-Hat-Hacker und IT-Security-Dienstleister. Kontaktdaten und mehr Informationen: <https://hansesecure.de/>

3.2

Die Allgemeinen Geschäftsbedingungen des Kunden werden nicht anerkannt, soweit die Parteien nicht ausdrücklich etwas anderes in Textform geregelt haben.

3.3

Für alle Verträge zwischen den Parteien findet das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts Anwendung. Die gesetzlichen Vorschriften zur Beschränkung der Rechtswahl und zur Anwendbarkeit zwingender Vorschriften insbesondere des Staates, in dem der Kunde als Verbraucher seinen gewöhnlichen Aufenthalt hat, bleiben unberührt.

3.4

Diese AGB und der Vertrag über die Auftragsverarbeitung (Art. 28 DSGVO; Anlage 1) werden in jeden Vertrag einbezogen, den die Parteien schließen. Auf Verlangen des Kunden kann darüber hinaus eine Geheimhaltungsvereinbarung (Anlage 2) geschlossen werden.

4 BEGRIFFSBESTIMMUNGEN

„System“: Der Begriff des „Systems“ beschreibt diejenigen abgrenzbaren oder bestimmbar Bestandteile der EDV-Infrastruktur des Kunden, die von diesem als Testumgebung für den Dienstleister ausgewählt wurden. Bei der Erbringung seiner Leistungen wird sich der Dienstleister auf die EDV-Geräte fokussieren, die zum „System“ gehören.

5 PENETRATIONSTESTS

5.1 LEISTUNGSBESCHREIBUNG

5.1.1

Bei einem Penetrationstest wird der Dienstleister vom Kunden im Rahmen eines Dienstvertrags beauftragt, zu versuchen, von innerhalb oder außerhalb der IT-Infrastruktur des Kunden in eine von ihm betriebene oder genutzte EDV-Anlage („System“) einzudringen. Ein Erfolg ist ausdrücklich nicht geschuldet, da nicht vorhergesagt werden kann, ob eine Penetration der Systemsicherheit gelingen wird oder ob alle Schwachstellen ermittelt werden können. Mit automatisierten und manuell gesteuerten Angriffen wird ermittelt, ob z.B. das Erlangen der Rechte des Domain-Administrators, der Zugriff auf Kundendaten oder die Verschlüsselung von Kundendaten möglich wäre. Durch Penetrationstests sollen Schwachstellen des Systems aufgedeckt werden. Durch die damit einhergehende Identifikation der Schwachstellen des kritischen Systems wird der Kunde in die Lage versetzt, die Schwachstellen seines Systems zu erkennen und durch technische und organisatorische Maßnahmen zu beheben, um sein System vor unberechtigten Zugriffen Dritter zu schützen. Zur Leistungserbringung werden Funktionen, Software und Methoden nach dem gegenwärtigen Stand der Technik verwendet und fachmännisch ausgeführt.

5.1.2

Folgende Leistungen sind bei Penetrationstests ausdrücklich nicht enthalten:

5.1.2.1

Der Dienstleister nimmt keine Konfigurationen an dem System mit dem Ziel vor, Schwachstellen zu beheben oder das System zu härten. Härtung bedeutet, dass vorhandene Sicherheitsmaßnahmen optimiert werden, um einen noch höheren Grad an Sicherheit zu erreichen. Die Konfiguration kann als Zusatzdienstleistung gesondert vereinbart werden.

5.1.2.2

Der Dienstleister wird keine Meldungen an Behörden oder sonstige Dritte unternehmen. Dies gilt auch für den Fall, dass der Dienstleister z.B. einen erfolgten oder gerade stattfindenden IT-Sicherheitsvorfall bei der Erbringung seiner Leistung entdecken sollte. Er wird den Kunden aber unverzüglich darüber informieren.

5.1.2.3

Der Dienstleister leistet keine Rechtsberatung, Datenschutzberatung oder IT-Forensik. Diese Zusatzdienstleistungen können aber ggf. über Kooperationspartner erbracht werden.

5.1.2.4

Der Abschlussbericht der Penetrationstests beinhaltet nicht alle in dem System auffindbaren Schwachstellen, sondern dokumentiert lediglich eine Momentaufnahme an dem Tag der Leistungserbringung ohne die Gewähr, dass alle möglicherweise im System enthaltenen Schwachstellen vom Dienstleister aufgefunden werden können.

5.1.2.5

Der Dienstleister führt in der Regel nur Abschlussgespräche mit Mitarbeitern, aber keine Schulungen für Administratoren oder IT-Sicherheitsdienstleister des Kunden durch.

5.1.2.6

Für die Leistungen des „Schwachstellen-Scans“ und des „Mail-Audits“ gelten die vorstehend geregelten Vorschriften entsprechend.

5.2 SCOPE UND SYSTEM

Der Kunde teilt dem Dienstleister bei Auftragserteilung oder im Rahmen des Kickoff-Meetings mit, welche strategischen und operativen Ziele (fortan „Scope“ genannt) er mit dem Penetrationstest verfolgt und gibt konkret an, welche Bestandteile seiner EDV-Anlage an welchem Ort („System“) getestet werden sollen.

Änderungs- oder Ergänzungswünsche des Kunden, die nach der Angebotserstellung dem Dienstleister, z.B. im Kickoff-Meeting, mitgeteilt werden, wird er per Textform bestätigen (§ 346 HGB).

5.3 RISIKOHINWEISE

Die Parteien sind sich einig, dass Penetrationstests ein System und den Betriebslauf im Unternehmen des Kunden beeinträchtigen können.

5.3.1

Der Dienstleister hat den Kunden über das Risiko informiert, dass bei der Durchführung des Penetrationstests das System und/oder die darauf gespeicherten Daten oder Anwendungen beeinträchtigt werden können. Insbesondere bei sog. „Denial of Service“-Angriffen kann es passieren, dass das System ausfällt und infolge der Tests zeitweise nicht zur Verfügung steht oder dass darin gespeicherte Daten verlorengehen. Zudem besteht das Risiko, dass Antworten der Dienste durch den Penetrationstest verzögert werden.

5.3.2

Der Dienstleister hat den Kunden auch darüber informiert, dass eine Beeinträchtigung des Systems rechtliche Konsequenzen für den Kunden nach sich ziehen kann.

5.4 PFLICHTEN DES KUNDEN

5.4.1

Der Kunde versichert, dass er die Risikohinweise in diesem Vertrag gelesen hat und erklärt, dass er bereit ist, sämtliche Risiken einzugehen und eventuelle, durch den Dienstleister verursachte Schäden auf eigene Kosten zu beseitigen. Der Dienstleister haftet auf Schadenersatz nur in dem in Ziff. 11 geregelten Umfang.

5.4.2

Der Kunde garantiert, dass er alle Daten des Systems vor der Durchführung des Penetrationstests derart gesichert hat, dass er im Falle eines Datenverlusts diese vollständig wiederherstellen kann („Backup“). Er stellt auch sicher, dass er alle vom Dienstleister empfohlenen Vorbereitungen getroffen hat, damit dieser seine Leistungen ordnungsgemäß erbringen kann.

5.4.3

Der Kunde versichert ausdrücklich gegenüber dem Dienstleister und dessen Mitarbeitern und Erfüllungsgehilfen, dass die Systeme, die ihm vom Kunden in Textform benannt wurden, ausschließlich vom Kunden selbst betrieben und genutzt werden und Dritte von einer Beeinträchtigung der gegenständlichen Systeme oder mit diesen verbundenen Systemen nicht betroffen sein werden.

5.4.4

Soweit das System nicht ausschließlich durch den Kunden selbst genutzt wird oder in Verbindung mit Systemen Dritter genutzt wird, versichert der Kunde ausdrücklich, dass alle davon betroffenen Personen zugestimmt haben, dass ihre personenbezogenen Daten im Rahmen des Penetrationstests verarbeitet werden.

5.4.5

Der Kunde wird alle Personen, die im Rahmen der Penetrationstests des Dienstleisters als datenschutzrechtlich betroffene Personen gelten, nach Maßgabe von Art. 13, 14 DSGVO und Ziff. 12 über die Datenverarbeitung unterrichten (Datenschutzerklärung).

5.4.6

Der Kunde versichert auch, dass er die betroffenen Dritten, z.B. Administratoren oder IT-Sicherheitsdienstleister, über die möglichen Auswirkungen des Penetrationstests informiert hat und diese mit der Vornahme des Penetrationstests einverstanden sind.

Widersprechen betroffene Dritte gegenüber dem Dienstleister dem Penetrationstest auf das gegenständliche System, ist der Dienstleister berechtigt, den Penetrationstest dieses Systems unverzüglich zu beenden. Der Kunde hat für den hierdurch entstehenden Schaden einzustehen. Der Kunde hält den Dienstleister vollumfänglich schadlos, sollte der Dienstleister von Dritten in Anspruch genommen werden, weil der Kunde die erforderlichen Zustimmungen Dritter nicht rechtzeitig eingeholt hat oder wenn durch den Penetrationstest des Systems Schäden bei Dritten entstehen. Dies gilt auch für Aufwand, der dem Dienstleister dadurch entsteht, dass Strafverfolgungs- oder Aufsichtsbehörden gegen ihn wegen vermeintlicher Rechtsverletzungen durch die Penetrationstests Ermittlungen eingeleitet haben, weil er von Personen, die über den Penetrationstest nicht informiert waren, angezeigt wurde. Ziff. 5 gilt auch für Schäden, welche Dritten aufgrund der Beeinträchtigung von mit dem System verbundenen Systemen entstehen. Diese Pflicht zur Schadloshaltung entfällt bei grob fahrlässigem oder vorsätzlichem Handeln des Dienstleisters, seinen Vertretern oder Erfüllungsgehilfen oder bei Verletzung von Kardinalpflichten durch den Dienstleister.

6 PHISHINGTEST

6.1 LEISTUNGSBESCHREIBUNG

6.1.1

Im Rahmen der per E-Mail-Versand geführten Phishing-Kampagne werden Phishing-Angriffe auf Mitarbeiter des Betriebs des Kunden realitätsgetreu simuliert. Allerdings enthalten die Test-Phishing-E-Mails keinen Schadcode, sondern Links, die -wenn man sie anklickt- die Empfänger der E-Mails auf eine Internetseite mit Informationen über die Simulation enthalten. Die Empfänger werden auf diese Weise über den simulierten Angriff und die möglichen Folgen unterrichtet, die der Mausklick gehabt hätte, wenn es keine Simulation gewesen wäre. Der Dienstleister erfasst das Nutzerverhalten im Rahmen der Simulation.

6.1.2

Einzelheiten zur Phishing-Kampagne, insbesondere die Laufzeit, die Verwendung von Mustern, Frequenz und Schwierigkeitsgrad, vereinbaren die Parteien auf der Basis des Leistungsverzeichnisses des Dienstleisters.

6.1.3

Zum Abschluss erhält der Kunde einen detaillierten Bericht darüber, wie wahrscheinlich Mitarbeiter des Betriebs des Kunden auf Links in Phishing-Emails klicken. Der Bericht enthält keine personenbezogenen Daten, insbesondere keine Information darüber, wer auf welche E-Mail geklickt hat. Der Bericht kann im Rahmen einer Präsentation besprochen werden.

6.1.4

Die Erbringung der Leistung „Phishing“ setzt voraus, dass der Kunde bestimmte System- und Testbedingungen zu Beginn und während des vereinbarten Leistungszeitraums gewährleistet und alle Mitwirkungspflichten erfüllt, die er dazu in Form einer Anleitung erhält.

6.1.5

Der Kunde wird alle Personen, die im Rahmen des Phishing-Tests des Dienstleisters als datenschutzrechtlich betroffene Personen gelten, nach Maßgabe von Art. 13, 14 DSGVO und Ziff. 12 über die Datenverarbeitung unterrichten (Datenschutzerklärung).

6.1.6

Folgende Leistungen bei Phishing-Tests sind ausdrücklich nicht enthalten:

6.1.6.1

Der Dienstleister wird im Rahmen des Phishing-Tests keine Sicherheitsüberprüfung, z.B. die in Ziff. III genannten Penetrationstests oder Schwachstellen-Scans, durchführen.

6.2 SCOPE UND SYSTEM

Der Kunde teilt dem Dienstleister bei Auftragserteilung oder im Rahmen des Kickoff-Meetings mit, welche strategischen und operativen Ziele (fortan „Scope“ genannt) er mit dem Phishing-Test verfolgt und gibt konkret an, welche Bestandteile seiner EDV-Anlage an welchem Ort bzw. welche Teile der Belegschaft („System“) getestet werden sollen.

Zur Anmeldung der Empfänger seiner Belegschaft erhält der Kunde vom Dienstleister ein Excel-Formular. Der Dienstleister beginnt mit der Erbringung seiner Leistung, sobald er dieses Excel-Formular vollständig und richtig ausgefüllt erhalten hat.

Änderungs- oder Ergänzungswünsche des Kunden, die nach der Angebotserstellung dem Dienstleister, z.B. im Kickoff-Meeting, mitgeteilt werden, wird er per Textform bestätigen (§ 346 HGB).

6.3 RISIKOHINWEISE UND PFLICHTEN

Wenn der Kunde die Sicherheitseinstellungen seines Mailservers verändert, ist es nicht ausgeschlossen, dass er nicht nur Test-E-Mails des Dienstleisters, sondern auch echte Phishing-E-Mails mit Schadcode empfängt, die von Mitarbeitern angeklickt werden. Der Kunde erklärt, dass er diesen Gefahrenhinweis verstanden hat und sich an die Anleitung des Dienstleisters zur Vorbereitung des Phishing-Tests halten wird.

7 EINWILLIGUNG BZGL. STRAFTATBESTÄNDEN (HACKER-PARAGRAPHEN)

Der Dienstleister weist den Kunden darauf hin, dass sich die beauftragten Leistungen als Straftaten u.a. wegen der Verletzung des Briefgeheimnisses (§ 202 StGB), des Ausspähens von Daten (§ 202 a StGB), des Abfangens von Daten (§ 202 b StGB), des Vorbereitens des Ausspähens und Abfangens von Daten (§ 202 c StGB), der Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB), der Fälschung beweiserheblicher Daten (§ 269 StGB) oder der Datenveränderung (§ 303 a StGB) darstellen können.

In Bezug auf diese Unterrichtung erklärt sich der Kunde mit der Vereinbarung dieses Vertrags ausdrücklich mit der Vorbereitung und Durchführung des Angebots durch den Dienstleister einverstanden. Diese Einwilligung entfaltet ausdrücklich auch Wirkung gegenüber den vom Dienstleister eingesetzten Mitarbeitern und Erfüllungsgehilfen, ganz gleich, ob diese natürliche oder juristische Personen sind.

8 VERTRAGSSCHLUSS UND LEISTUNGSÄNDERUNGEN

8.1

Zwischen den Parteien kommt ein Vertrag zustande, wenn der Kunde das vom Dienstleister erstellte Angebot annimmt. Die Annahme kann in Textform, z.B. per E-Mail, erklärt werden.

8.2

Wenn der Kunde nach der Annahme des Angebots Änderungswünsche in Bezug auf den Scope, das System oder andere Leistungsgegenstände äußert, wird der Dienstleister diese Leistungsänderung oder Leistungserweiterung mit einem kaufmännischen Bestätigungsschreiben bestätigen.

8.3

Weitere Einzelheiten zu Penetrationstests oder Phishing-Tests sind im Leistungsverzeichnis enthalten, die in diese AGB als Vertragsbestandteil einbezogen werden.

8.4

Änderungs- oder Ergänzungswünsche des Kunden, insbesondere in Bezug auf Scope, System, Zeitplan oder Zielsetzung, führen zu einer entsprechenden Anpassung der Vergütung und des Leistungszeitraums.

Der Dienstleister ist berechtigt, die Umsetzung von Änderungen von einer vorherigen Bestätigung des Mehraufwands abhängig zu machen.

Erfolgt die Umsetzung von Änderungen auf Wunsch des Kunden ohne vorherige ausdrückliche Vereinbarung, gilt eine Vergütung nach den jeweils gültigen Tagessätzen des Dienstleisters als vereinbart.

9 VERGÜTUNG UND ZAHLUNGSBEDINGUNGEN

9.1

Leistungen des Dienstleisters werden nach Aufwand oder zum Pauschalpreis vergütet. Die Abrechnung nach Aufwand erfolgt hierbei nach tatsächlich erbrachten Personentagen und Geschäftszeiten. Leistungen, die außerhalb der Geschäftszeiten

erbracht werden sollen oder müssen, werden mit einem Netto-Aufschlag von 25% für den angefallenen Aufwand abgerechnet.

9.2

Ein Personentag hat acht (8) Stunden. Mehr- oder Minderleistungen je Personentag werden anteilig vergütet.

9.3

Der Dienstleister hat darüber hinaus Anspruch auf Erstattung der für die Erbringung der Leistungen erforderlichen und nachgewiesenen Auslagen einschließlich der Reisekosten.

9.4

Die erbrachten Leistungen werden monatlich nach Leistungserbringung oder pauschal in Rechnung gestellt. Rechnungen sind mit Zugang zur Zahlung fällig. Rechnungen des Dienstleisters enthalten Angaben zur Anzahl der durch jeden eingesetzten Mitarbeiter geleisteten Arbeitstage unter Angabe des Leistungsdatums, des Tagessatzes des jeweiligen Mitarbeiters sowie eine Beschreibung der abgerechneten Leistungen und zu erstattenden Auslagen.

9.5

Soweit nicht ausdrücklich etwas anderes vereinbart ist, verstehen sich alle Preisangaben zuzüglich der jeweils geltenden Umsatzsteuer.

9.6

Bei Zahlungsverzug ist der Dienstleister berechtigt, für den zusätzlichen administrativen Aufwand eine pauschale Bearbeitungsgebühr in angemessener Höhe zu erheben.

10 VERTRAGSLAUFZEIT UND KÜNDIGUNG

10.1

Der Vertrag über die Erbringung einer Leistung beginnt mit dem Vertragsschluss. Diese AGB, die Anlagen und die Leistungsverzeichnisse werden in alle Verträge als Vertragsbestandteil einbezogen. Der Vertrag endet mit Ablauf der im Auftrag bestimmten

Leistungszeit oder in dem Zeitpunkt, in dem die Leistung vollständig erbracht ist, ohne dass es einer Kündigung bedarf.

10.2

Die ordentliche Kündigung durch den Kunden ist für die Laufzeit des Vertrags ausgeschlossen. Das Recht beider Parteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

10.3

Der Dienstleister ist berechtigt, den Vertrag mit einer Frist von 14 Kalendertagen ordentlich zu kündigen, sofern berechnete Interessen dies erfordern, insbesondere bei fehlender Mitwirkung des Kunden, Zahlungsverzug oder unzumutbarer Projektfortführung. Bereits erbrachte Leistungen sind in jedem Fall zu vergüten.

11 HAFTUNG

11.1

Der Dienstleister haftet – außer bei Vorsatz, grober Fahrlässigkeit, bei der Verletzung von Leben, Körper oder Gesundheit sowie bei Ansprüchen nach dem Produkthaftungsgesetz – nur bei der Verletzung wesentlicher Vertragspflichten. Bei leicht fahrlässiger Verletzung wesentlicher Vertragspflichten ist die Haftung auf den bei Vertragsschluss vorhersehbaren, vertragstypischen Schaden begrenzt. Wesentliche Vertragspflichten sind nur solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf.

11.2

Soweit gesetzlich zulässig, ist die Haftung des Dienstleisters für sämtliche Schäden aus und im Zusammenhang mit dem jeweiligen Vertrag der Höhe nach auf den Netto-Auftragswert des jeweiligen Einzelauftrags, maximal jedoch auf 100.000 EUR, begrenzt.

Dies gilt nicht bei Vorsatz, grober Fahrlässigkeit, bei Verletzung von Leben, Körper oder Gesundheit sowie in den Fällen zwingender gesetzlicher Haftung.

11.3

Nicht zu den wesentlichen Vertragspflichten gehören insbesondere die vollständige Aufdeckung sämtlicher Schwachstellen, die Verhinderung von Sicherheitsvorfällen oder die Erzielung eines bestimmten Test- oder Prüfergebnisses.

12 DATENSCHUTZHINWEISE

12.1 ALLGEMEINE DATENSCHUTZHINWEISE

Im Rahmen dieses Vertrags verarbeitet der Dienstleister personenbezogene Daten, v.a. Namen, Adressen, Kontaktdaten, ggf. Bankdaten des Kunden und ggf. von dessen Mitarbeitern, um Verträge aufgrund dieser AGB einzugehen und zu erfüllen, allerdings nur soweit dies erforderlich ist. Diese Datenverarbeitung wird auf Art. 6 Abs. 1 S. 1 lit. b DSGVO gestützt. Diese personenbezogenen Daten werden ferner zur Korrespondenz, Zahlungsabwicklung und ggf. zur Abwehr oder Geltendmachung von Forderungen verarbeitet, um berechnigte wirtschaftliche Interessen wahrzunehmen, Art. 6 Abs. 1 S. 1 lit. f DSGVO. Personenbezogene Daten, die im Rahmen eines Vertragsschlusses erhoben wurden, werden spätestens nach Ablauf der Aufbewahrungsfristen vernichtet. Rechnungsbelege werden 10 Jahre aufbewahrt. Betroffene Personen haben ein Recht auf Auskunft, Berichtigung, Einschränkung, Löschung, Datenübertragbarkeit, Widerruf einer Einwilligung und Widerspruch sowie ein Recht auf Beschwerde bei jeder Datenschutzaufsichtsbehörde. Anfragen und Anträge sind an den Dienstleister zu richten.

12.2 DATENVERARBEITUNG IM RAHMEN DER LEISTUNGSERBRINGUNG

Im Rahmen dieses Vertrags verarbeitet der Dienstleister personenbezogene Daten, v.a. Namen, Adressen, Kontaktdaten, ggf. Bankdaten des Kunden und ggf. von dessen Mitarbeitern, um Verträge aufgrund dieser AGB einzugehen und zu erfüllen, allerdings nur soweit dies erforderlich ist. Diese Datenverarbeitung wird auf Art. 6 Abs. 1 S. 1 lit. b DSGVO gestützt. Diese personenbezogenen Daten werden ferner zur Korrespondenz, Zahlungsabwicklung und ggf. zur Abwehr oder Geltendmachung von Forderungen verarbeitet, um berechnigte wirtschaftliche Interessen wahrzunehmen, Art. 6 Abs. 1 S. 1 lit. f DSGVO. Personenbezogene Daten, die im Rahmen eines Vertragsschlusses erhoben wurden, werden spätestens nach Ablauf der Aufbewahrungsfristen vernichtet. Rechnungsbelege werden 10 Jahre aufbewahrt. Betroffene Personen haben ein Recht

auf Auskunft, Berichtigung, Einschränkung, Löschung, Datenübertragbarkeit, Widerruf einer Einwilligung und Widerspruch sowie ein Recht auf Beschwerde bei jeder Datenschutzaufsichtsbehörde. Anfragen und Anträge sind an den Dienstleister zu richten.

12.3 AUFTRAGSVERARBEITUNG

Der Kunde bleibt nach Maßgabe von Art. 4 Nr. 2 DSGVO allein verantwortlich für die Verarbeitung von allen personenbezogenen Daten, die von Penetrationstests betroffen sind. Der Dienstleister ist lediglich Auftragsverarbeiter im Sinne von Art. 28 DSGVO. Dazu schließen die Parteien den in der Anlage beigefügten Vertrag über die Auftragsverarbeitung.

13 GEHEIMHALTUNGS- UND REFERENZKLAUSEL

13.1

Der Dienstleister wird vertrauliche Informationen im Sinne von § 2 Nr. 1 Geschäftsgeheimnisgesetz vertraulich behandeln. Näheres ist der Vertraulichkeitsvereinbarung geregelt, die als Bestandteil des Vertrags einbezogen wird.

13.2

Der Dienstleister ist berechtigt, die Firma, das Unternehmenskennzeichen oder eine Marke des Kunden zu verwenden, um damit unter der Rubrik „Referenzen“ oder „Referenzkunden“ auf seiner Internetseite zu werben. Darüber hinaus wird der Dienstleister keine Informationen über die Erbringung von Tätigkeiten für den Kunden veröffentlichen oder in sonstiger Weise preisgeben.

14 ABWERBUNG VON MITARBEITERN

Der Kunde verpflichtet sich, während der Laufzeit des Vertrags sowie für einen Zeitraum von zwölf (12) Monaten nach dessen Beendigung keine Mitarbeiter oder freien Mitarbeiter des Dienstleisters, die im Rahmen der Leistungserbringung eingesetzt wurden, unmittelbar oder mittelbar aktiv abzuwerben oder durch Dritte abwerben zu lassen. Dies gilt auch für die unmittelbare oder mittelbare Begründung eines Vertrags-, Arbeits- oder freien Mitarbeiterverhältnisses infolge einer solchen Abwerbung.

Im Falle eines Verstoßes verpflichtet sich der Kunde zur Zahlung einer Vertragsstrafe in Höhe von **100.000 EUR** oder dem entgangenen Umsatz des Dienstleisters für einen Zeitraum von bis zu sechs (6) Monaten auf Basis des zuletzt vereinbarten Tagessatzes des betroffenen Mitarbeiters – je nachdem, welcher Betrag höher ist.

Maßgeblich ist der Zeitraum, der typischerweise erforderlich ist, um einen gleichwertigen Ersatz für den betroffenen Mitarbeiter zu rekrutieren und einzuarbeiten.

Die Geltendmachung eines darüber hinausgehenden Schadens bleibt vorbehalten. Eine verwirkte Vertragsstrafe wird auf einen etwaigen Schadensersatz angerechnet.

Als Abwerbung gilt auch die Einschaltung Dritter (z. B. Personalvermittler) oder die gezielte Ansprache über berufliche Netzwerke, sofern diese im Zusammenhang mit der Zusammenarbeit steht.

Sollte die Vertragsstrafe nach Maßgabe zwingenden Rechts ganz oder teilweise unwirksam sein, bleibt die Verpflichtung des Kunden zum Ersatz des tatsächlich entstandenen Schadens unberührt.

15 NUTZUNGSRECHTE UND GEISTIGES EIGENTUM

Sämtliche im Rahmen der Leistungserbringung erstellten Inhalte, insbesondere Berichte, Analysen, Konzepte und Methoden, bleiben geistiges Eigentum des Dienstleisters.

Der Kunde erhält ein einfaches, nicht übertragbares Nutzungsrecht zur internen Verwendung.

Eine Weitergabe an Dritte oder kommerzielle Nutzung bedarf der vorherigen Zustimmung des Dienstleisters.

16 KEINE ERFOLGSGARANTIE

Der Dienstleister übernimmt keine Garantie, Zusicherung oder sonstige Gewähr dafür, dass die Systeme des Kunden nach Durchführung der Leistungen frei von Sicherheitslücken sind oder dass zukünftige Angriffe, Sicherheitsvorfälle oder Beeinträchtigungen verhindert werden.

17 SCHLUSSBESTIMMUNGEN

17.1

Der Kunde ist zur Abtretung von Ansprüchen gegen den Auftraggeber an Dritte nur nach schriftlicher Zustimmung des Dienstleisters berechtigt. § 354a HGB bleibt unberührt.

17.2

Jede Vertragspartei darf nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen aufrechnen.

17.3

Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform.

17.4

Auf diesen Vertrag ist das deutsche Recht unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenverkauf vom 11.4.1980 (UN-Kaufrecht) anzuwenden.

17.5

Ausschließlicher Gerichtsstand ist München, sofern jede Partei Kaufmann oder juristische Person des öffentlichen Rechts ist oder keinen allgemeinen Gerichtsstand in Deutschland hat.

17.6

Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Die Vertragsparteien werden sich bemühen, anstelle der unwirksamen Bestimmung eine solche zu finden, die dem Vertragsziel rechtlich und wirtschaftlich am besten gerecht wird.

17.7

Sämtliche in diesem Vertrag genannten Anlagen sind verpflichtender Teil des Vertrags.