Allgemeine Geschäftsbedingungen für Dienstleistungen (AGB)

Gürtler & Roach Cybersecurity, GmbH
Leopoldstraße 31
80802 München
Tel: +49 89 614 65 283
www.gr-sec.com

1 Vertragsgegenstand - Geltungsbereich

1.1 Die Gürtler & Roach Cybersecurity, GmbH, Leopoldstraße 31, 80802 München, Germany (nachfolgend „*G&R Cybersecurity*“ genannt), erbringt für den Auftraggeber Dienstleistungen gemäß dem vertraglich festgelegten Leistungsumfang. G&R Cybersecurity erbringt die Dienstleistungen in eigener Verantwortung; für die dabei vom Auftraggeber angestrebten und erzielten Ergebnisse bleibt der Auftraggeber selbst verantwortlich.

1.2 Die geschuldeten Dienstleistungen werden entsprechend den im Vertrag genannten Leistungsbeschreibungen erbracht.

1.3 Die gefundenen Ergebnisse sind nur zum Zeitpunkt der erbrachten Leistung gültig.

1.4 Wegen eventueller Beschränkungen der zeitlichen, finanziellen und personellen Ressourcen wird Seitens G&R Cybersecurity nicht gewährleistet, dass alle vorhandenen Fehler gefunden werden.

1.5 Entgegenstehende oder abweichende AGB, oder sonstige Einschränkungen des Auftraggebers werden nicht Vertragsbestandteil, es sei denn, G&R Cybersecurity hat ihnen im Einzelfall vor Vertragsschluss ausdrücklich und in Textform zugestimmt.

1.6 Diese AGB gelten auch für alle künftigen gleichgelagerten Geschäftsbeziehungen, auch wenn sie nicht nochmals ausdrücklich vereinbart werden.

1.7 Im Einzelfall getroffene, individuelle Vereinbarungen mit dem Auftraggeber haben in jedem Fall Vorrang vor diesen AGB.

1.8 Sollten sich in den AGB und dem den AGB jeweils zugrundeliegenden Vertrag abweichende Bedingungen ergeben, so gilt im Zweifelsfall die Angabe des jeweiligen Vertrags.

2 Zustandekommen des Vertrages, Zeitpläne

2.1 Angebote von G&R Cybersecurity sind freibleibend, sofern nichts Abweichendes angegeben ist und 30 Tage ab Angebotsdatum gültig.

2.2 Ein Vertrag kommt mit der Annahme eines von G&R Cybersecurity schriftlich oder in Textform übermittelten Angebots durch den Auftraggeber oder mittels schriftlicher oder in Textform übermittelter Bestellung des Auftraggebers und Zugang einer entsprechenden Auftragsbestätigung von G&R Cybersecurity beim Auftraggeber zustande.

2.3 Die Vertragspartner vereinbaren für die Erbringung der Dienstleistungen Zeitpläne. Diese können im gegenseitigen Einvernehmen geändert werden.

3 Änderung der vereinbarten Dienstleistungen

3.1 Jeder der Vertragspartner kann beim anderen Vertragspartner in schriftlicher Form oder Textform Änderungen des vereinbarten Leistungsumfangs beantragen. Nach Erhalt eines Änderungsantrags wird der Empfänger die Änderung daraufhin überprüfen, ob und zu welchen Bedingungen diese durchführbar ist und dem Antragsteller die Zustimmung bzw. Ablehnung unverzüglich schriftlich oder in Textform mitteilen und gegebenenfalls begründen.

3.2 Erfordert ein Änderungsantrag des Auftraggebers eine umfangreiche Überprüfung, so kann der erforderliche Aufwand von G&R Cybersecurity berechnet werden.

3.3 Die für eine Überprüfung und/oder eine Änderung erforderlichen vertraglichen Anpassungen der vereinbarten Bedingungen und Dienstleistungen werden in einer Ergänzung zu diesem Vertrag vereinbart.

3.4 Solange die Zustimmung des Auftraggebers nicht vorliegt, setzt G&R Cybersecurity die Dienstleistungen nach dem bestehenden Vertrag fort. Jeder der Vertragspartner kann jedoch verlangen, dass die von der Änderung betroffenen Dienstleistungen bis zum Abschluss der Änderungsvereinbarung unterbrochen werden.

4 Mitwirkungspflicht des Auftraggebers

4.1 Der Auftraggeber wird alle einschließlich der nachfolgend aufgeführten angemessenen oder notwendigen Mitwirkungsleistungen rechtzeitig, vollständig und für G&R Cybersecurity kostenfrei erbringen.

4.2 Der Auftraggeber hat während der Ausführung der Dienstleistungen von G&R Cybersecurity stets dafür Sorge zu tragen, dass G&R Cybersecurity alle für die Ausführung ihrer Tätigkeit notwendigen Unterlagen rechtzeitig vorgelegt werden, G&R Cybersecurity alle Informationen erteilt werden und G&R Cybersecurity von allen Vorgängen und Umständen in Kenntnis gesetzt wird. Dies gilt auch für Unterlagen, Vorgänge und Umstände, die erst während der Tätigkeit von G&R Cybersecurity bekannt werden.

4.3 Der Auftraggeber benennt einen Ansprechpartner und einen Stellvertreter für G&R Cybersecurity, der als Koordinator die Gesamtverantwortung des Auftraggebers unter diesem Vertrag wahrnimmt und teilt G&R Cybersecurity dessen Kontaktdaten, sowie die Kontaktdaten des IT-Sicherheitsbeauftragten und des Datenschutzbeauftragten des Auftraggebers mit.

4.4 Der Auftraggeber benennt gegenüber G&R Cybersecurity einen Systemverantwortlichen mit Kontaktdaten. Der Systemverantwortliche und sein Stellvertreter sind neben der Geschäftsführung Ansprechpartner von G&R Cybersecurity in allen Fragen der Durchführung des Vertrages.

4.5 Der Auftraggeber ist selbst dafür verantwortlich das der IT-Sicherheitsbeauftragte und/oder der Datenschutzbeauftragte, sofern der Auftraggeber über einen solchen verfügt, informiert und in die Dienstleistungen der G&R Cybersecurity einbezogen ist.

4.6 Sofern der Auftraggeber Dienste bei einem Hoster ausgelagert hat, stellt der Auftraggeber sicher, dass auch dieser in den Vertrag einbezogen wird, sofern sich die vertraglich vereinbarten Dienstleistungen der G&R Cybersecurity auch auf diese Dienste beziehen.

4.7 Soweit es für die Erfüllung dieses Vertrages erforderlich ist, wird der Koordinator von G&R Cybersecurity notwendige Informationen übergeben und an Besprechungen mit G&R Cybersecurity teilnehmen.

4.8 Der Auftraggeber gewährt G&R Cybersecurity während der Vertragserfüllung – in dazu angemessenem Umfang – freien und gesicherten Zutritt zu seinen Geschäftsräumen und ist bereit, notwendige Arbeitsvoraussetzungen (wie z.B. Raum, Telefon und Datensichtgeräte) kostenfrei zur Verfügung zu stellen.

4.9 Sofern von G&R Cybersecurity für einen geplanten White-Box-Test angefordert, stellt der Auftraggeber alle notwendigen folgende Informationen, insbesondere nachfolgende Informationen rechtzeitig zur Verfügung

4.9.1 Netzpläne, in denen das Prüfobjekt innerhalb der Umgebung, in der es sich befindet, näher skizziert ist unter Angabe der verwendeten IP-Adressen und Darstellung anderer IT-Systemen und IT-Anwendungen zur Verfügung. Schnittstellen, welche auch von Externen zu erreichen sind (z.B. Anbindung ans Internet, WLAN, Netzwerkdosen), sollten besonders gekennzeichnet werden.

4.9.2 Rollen- und Berechtigungskonzepte

4.9.3 genaue Beschreibung des Prüfobjekts

4.9.4 Liste der IT-Systeme mit Beschreibung der Härtungsmaßnahmen

4.9.5 bei physical Audits stellt der Auftraggeber die termingerechte Verfügbarkeit von Mitarbeitern für Interviews sicher.

4.10 Der Auftraggeber übernimmt gegebenenfalls weitere Mitwirkungspflichten gemäß dem Leistungsumfang.

4.11 Der Auftraggeber stellt sicher, dass während der geplanten Zeiten der Tätigkeiten der G&R Cybersecurity an der IT des Auftraggebers nicht gleichzeitig Wartungsarbeiten an den betroffenen IT-Systemen durchgeführt werden.

4.12 Bei der Erfüllung dieses Vertrages ist G&R Cybersecurity davon abhängig, dass der Auftraggeber seine in diesem Vertrag genannten Mitwirkungspflichten erfüllt. Geschieht dies nicht, kann G&R Cybersecurity – unbeschadet weitergehender gesetzlicher Rechte – Änderungen des Zeitplanes und des Preises verlangen.

5 Verpflichtung des Auftraggebers zum Backup – Wichtig Hinweise an den Auftragsgeber

5.1 Vor Durchführung von Penetrationtests verpflichtet sich der Auftraggeber sämtliche durch G&R Cybersecurity zu prüfende Systeme und die damit in Verbindung stehenden Daten vollumfänglich durch ein externes Backup zu sichern. Darüber hinaus hat der Auftraggeber sämtliche notwendigen Sicherheitsmaßnahmen, auch diejenigen, die über ein Backup hinausgehen, vor Nutzung der Dienstleistung zu treffen, um die Systeme und Daten notfalls nach dem Penetrationtests wieder in den ursprünglichen Zustand zurück versetzen zu können. Der Auftraggeber verpflichtet sich weiterhin, für die regelmäßige vollständige Sicherung seiner Daten außerhalb des Zielsystems vor Durchführung des Penetrationstests selbst zu sorgen.

6 Zusicherung des Auftraggebers – Einholung von Zustimmungen – Haftung des Auftraggebers

6.1 Der Auftraggeber versichert, dass die Zielsysteme vom Auftraggeber allein betrieben und genutzt werden und Dritte von einer Beeinträchtigung der Zielsysteme oder mit diesen verbundenen Systemen nicht betroffen werden. Sofern die Zielsysteme nicht ausschließlich vom Auftraggeber genutzt versichert der Auftraggeber, dass er die Einwilligungen der betroffenen Dritten für einen Angriff auf das Zielsystem in Textform eingeholt hat und die betroffenen Dritte über die möglichen Auswirkungen der Penetrationtests nach dieser Vereinbarung belehrt hat.

6.2 Der Auftraggeber wird evtl. erforderliche weitere Zustimmungen Dritter z.B. nach DSGVO rechtzeitig einholen. Sofern vorhanden wird der Auftraggeber seinen Datenschutzbeauftragten / IT-Sicherheitsbeauftragten rechtzeitig über die geplanten Penetrationtests informieren.

6.3 Der Auftraggeber verpflichtet sich, sofern eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten im Sinne der EU Datenschutz-Grundverordnung (DSGVO) bestehen sollte, unverzüglich die zuständige Aufsichtsbehörde sowie gegebenenfalls die Betroffenen nach Maßgabe der DSGVO zu informieren.

6.4 Der Auftraggeber stellt die G&R Cybersecurity von sämtlichen Ansprüchen dritter Personen, die dritte Personen gegenüber G&R Cybersecurity, ihren gesetzlichen Vertretern und/oder Erfüllungsgehilfen im Fall einer schuldhaften Verletzung gegen die vorgenannten Verpflichtungen seitens des Auftraggebers oder eines anderen Dritten geltend machen, frei. Dies gilt auch für Schäden, welche Dritten aufgrund der Beeinträchtigung von mit dem Zielsystem verbundenen Systemen entstehen. Der Auftraggeber übernimmt dabei sämtliche Kosten und Gebühren für die notwendige rechtliche Verfolgung in der gesetzlichen Höhe, sowie sämtliche Schäden, Verluste und Ausgaben, insoweit die Rechtsverletzung durch den Auftraggeber zu vertreten ist. Vorstehendes gilt nicht bei grob fahrlässigem oder vorsätzlichem Handeln von G&R Cybersecurity oder bei Verletzung von Kardinalpflichten (wesentlichen Vertragspflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertraut und vertrauen darf) oder im Falle der Verletzung von Leben, Körper oder Gesundheit.

7 Abbruch des Penetrationstests – Ende des Penetrationstests

7.1 Der Auftraggeber hat jederzeit das Recht den Penetrationtest abzubrechen. Hierzu genügt eine Mitteilung in Textform durch die Geschäftsleitung oder den Systemverantwortlichen des Auftraggebers an G&R Cybersecurity.

7.2 G&R Cybersecurity ist selbst berechtigt und verpflichtet dem Angriff auf das Zielsystem unverzüglich einzustellen, sofern G&R Cybersecurity von betroffenen Dritten eine Mitteilung über einen unberechtigten Angriff auf dessen Systeme erfährt. Der Auftraggeber, der einen Angriff auf diese Zielsysteme beauftragt hat, hat für den hierdurch entstehenden Schaden einzustehen.

7.3 Bei Auffinden von eindeutig privaten oder inkriminierten Daten wird G&R Cybersecurity den Penetrationstest in diesem Bereich nicht weiter fortführen und umgehend einstellen. Der Abbruch ist im Abschlussbericht ohne Aufführung der Daten zu dokumentieren.

7.4 Nach Abschluss des Penetrationstests wird G&R Cybersecurity sämtliche Daten des Zielsystems des Auftraggebers, die während der praktischen Tests bei G&R Cybersecurity gespeichert worden sind, oder die G&R Cybersecurity während des Tests eventuell aus dem System des Auftraggeber erhalten hat, unverzüglich vollständig unwiederbringlich bei sich löschen.

8 Kosten bei Abbruch und Inaktivität

8.1 Sollte der Vertrag und damit die Leitungen von G&R Cybersecurity vorzeitig durch den Auftraggeber abgebrochen werden, oder wird für einen Zeitraum von drei Monaten kein Fortschritt mehr gemessen am vereinbarten Meilensteinplan erzielt (‚Inaktivität‘), so werden die Tätigkeiten und Aufwände von G&R Cybersecurity, die nicht bereits durch ggfs geleistete Vorauszahlungen des Auftraggebers abgedeckt sind, bis maximal zum Gesamtvolumen des Projekts zum Monatsende abgerechnet.

8.2 Im Fall von Inaktivität wird durch die Rechnungsstellung der Vertrag nicht automatisch abgebrochen oder beendet.

9 Hinweis auf Gefahren des Penetrationstests

9.1 Penetrationtests gehen immer mit einem unvermeidbaren Risiko einher. Eine Beschränkung auf Testmethoden, mit denen keinerlei Risiko einhergeht, ist nicht zu empfehlen, da die Aussagekraft zu gering wäre.

9.2 Der Auftraggeber wird ausdrücklich darauf hingewiesen, dass durch Penetrationtests Schäden am bestehenden System auftreten können. Im Rahmen von Penetrationtests kann es z.B. vorkommen, dass die Zielsysteme ausfallen und / oder Dienste zeitweise nicht mehr zur Verfügung stehen oder beeinträchtigt werden. Insbesondere können durch Penetrationtests Beeinträchtigungen und Veränderungen nur durch Wiederherstellungs-Backups, oder durch teilweise umfangreiche

Nachbearbeitung durch den Auftraggeber behoben werden können. Darüber hinaus besteht auch die Gefahr eines Verlustes von Daten des Zielsystems oder Daten.

10 Rechte an den Arbeitsergebnissen

10.1 Rechte an Arbeitsergebnissen, wie z.B. Auswertungen, Planungsunterlagen, Berichte, Dokumentationen, Zeichnungen und ähnliche Materialien, die dem Auftraggeber gemäß dem vereinbarten Leistungsumfang in schriftlicher, maschinenlesbarer und/oder anderer Darstellungsform übergeben werden, gehören, vorbehaltlich der nachstehenden Bestimmungen, dem Auftraggeber.

10.2 Sämtliche Rechte an von G&R Cybersecurity eingebrachten Grundlagen einschließlich der Rechte an Arbeitsunterlagen verbleiben bei G&R Cybersecurity.

10.3 Über Ideen, Konzeptionen, Know-how und Techniken, die von G&R Cybersecurity oder gemeinschaftlich mit dem Auftraggeber entwickelt werden, kann jeder Vertragspartner frei verfügen. Erfindungen, die im Rahmen dieses Vertrages durch G&R Cybersecurity gemacht werden sowie darauf erteilte Schutzrechte stehen G&R Cybersecurity zu. Der Auftraggeber erhält jedoch an den Erfindungen von G&R Cybersecurity, die im Rahmen dieses Vertrages entstanden sind, eine nicht ausschließliche, unwiderrufliche, gebührenfreie, weltweite Lizenz. Gemeinschaftliche Erfindungen sowie darauf erteilte Schutzrechte stehen beiden Vertragspartnern zu und jeder dieser Vertragspartner kann Lizenzen erteilen oder Rechte einräumen oder übertragen, ohne den anderen Vertragspartner zu unterrichten oder Zahlungen an ihn zu leisten.

10.4 G&R Cybersecurity ist durch diesen Vertrag nicht gehindert, Materialien zu entwickeln und Dritten zur Nutzung zu überlassen und hieran Rechte einzuräumen, die den an den Auftraggeber übergebenen Materialien ähnlich sind. Bei der Entwicklung von Materialien für Dritte wird G&R Cybersecurity jedoch die in Erfüllung dieses Vertrages ausschließlich und unmittelbar für den Auftraggeber geschaffenen Arbeitsergebnisse weder ganz noch teilweise kopieren.

11 Personal

11.1 G&R Cybersecurity benennt einen Ansprechpartner für den Koordinator des Auftraggebers zur gegenseitigen Abstimmung und Klärung aller Fragen, die sich im Verlauf der Leistungserbringung ergeben.

11.2 Die Vertragspartner sind während der Leistungserbringung für die Beaufsichtigung, Steuerung, Kontrolle und Entlohnung ihrer jeweils eingesetzten eigenen Mitarbeiter verantwortlich.

11.3 Mitarbeiter von G&R Cybersecurity treten in kein Arbeitsverhältnis zum Arbeitgeber ein.

12 Vertrauliche Daten, Datenschutz

12.1 Die Vertragspartner verpflichten sich, alle ihnen im Rahmen des Vertrages zugänglich gemachten, sowie bei Gelegenheit der Zusammenarbeit erlangten Informationen über Angelegenheiten der anderen Partei, die als vertraulich gekennzeichnet sind oder die als vertraulich bezeichnet werden oder die aus Sicht eines objektiven Beobachters als vertraulich erkennbar sind sowie Geschäfts- und Betriebsgeheimnisse, insbesondere, aber nicht ausschließlich, Informationen, Daten, Ideen, Konzepte und Businessmodelle, vertraulich zu behandeln. Den Vertragspartnern ist es untersagt, vertrauliche Informationen ohne schriftliche Einwilligung der anderen Vertragspartei zu einem anderen als dem zur vertragsgemäßen Aufgabenerfüllung vorgesehenen Zweck zu verwerten, Dritten zugänglich zu machen, oder sonst zu nutzen.

12.2 Beide Vertragspartner verpflichten sich, die Geheimhaltungspflicht sämtlichen Angestellten und/oder Dritten (freie Mitarbeiter etc.), die Zugang zu den vorbezeichneten Geschäftsvorgängen haben, aufzuerlegen.

12.3 Die Geheimhaltungspflicht gilt nicht für Informationen, die der jeweils anderen Partei bei Abschluss des Vertrags bereits bekannt waren, die zum Zeitpunkt der Weitergabe durch die offenlegende Partei bereits veröffentlicht waren, ohne dass dies von einer Verletzung der Vertraulichkeit durch die jeweils andere Partei herrührt, die die jeweils andere Partei ausdrücklich schriftlich zur Weitergabe freigegeben hat, die die jeweils andere Partei rechtmäßig und ohne die Vertraulichkeit betreffende Einschränkung aus anderen Quellen erhalten hat, sofern die Weitergabe und Verwertung dieser vertraulichen Informationen weder vertragliche Vereinbarungen noch gesetzliche Vorschriften oder behördliche Anordnungen verletzen, die die jeweils andere Partei selbst ohne Zugang zu den vertraulichen Informationen des Auftraggebers entwickelt hat, die aufgrund gesetzlicher Auskunfts-, Unterrichtungs- und/oder Veröffentlichungspflichten oder behördlicher Anordnung offen gelegt werden müssen. Soweit zulässig, wird die hierzu verpflichtete Partei die jeweils andere Partei hierüber so früh wie möglich informieren und sie bestmöglich dabei unterstützen, gegen die Pflicht zur Offenlegung vorzugehen.

12.4 G&R Cybersecurity verpflichtet sich, weder über die vorgefundenen Sicherheitsmängel, noch über die Organisationsstrukturen und die Struktur der überprüften IT-Systeme, noch über gesichtetes Firmen-Know-How des Auftraggebers gegenüber Dritten zu kommunizieren.

12.5 Die Verpflichtung zur Geheimhaltung besteht nach Beendigung des Vertrags fort.

12.6 Die Vertragspartner verpflichten sich, die Bestimmungen der DS-GVO einzuhalten. Soweit durch den Auftragnehmer eine Verarbeitung personenbezogener Daten erfolgt, werden die Parteien hierfür eine gesonderte Vereinbarung abschließen.

13 Vertragsdauer – Kündigung

13.1 Der Vertrag endet nach Erbringung der vereinbarten Dienstleistungen. Eine Verlängerung des Vertrages kann jederzeit vor seiner Beendigung zu den jeweils gültigen Preisen und Bedingungen von G&R Cybersecurity schriftlich oder in Textform vereinbart werden.

13.2 Im Übrigen beträgt die Kündigungsfrist vier Wochen zum Monatsende, sofern nicht im Einzelfall abweichend vereinbart.

13.3 Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

13.4 Jede Kündigung bedarf zu Ihrer Wirksamkeit der Schriftform.

14 Vergütung und Zahlungsbedingungen

14.1 Alle Preise verstehen sich zuzüglich der jeweils geltenden gesetzlichen Umsatzsteuer.

14.2 Die Dienstleistungen von G&R Cybersecurity und ggf. zusätzlichen Kosten (Reisekosten, Material, Versandkosten, usw.) werden entsprechend der im Angebot bzw. Vertrag aufgeführten Zahlungsbedingungen in Rechnung gestellt.

14.3 Rechnungen sind bei Erhalt sofort ohne Abzug zahlbar.

14.4 Ist der Rechnungsbetrag nicht innerhalb von 30 Tagen nach dem Rechnungsdatum bei G&R Cybersecurity eingegangen, ist G&R Cybersecurity berechtigt, Verzugszinsen in gesetzlicher Höhe geltend zu machen.

15 Haftung – Haftungsbeschränkung

15.1 G&R Cybersecurity haftet im Falle von Arglist, Vorsatz oder grober Fahrlässigkeit nach Maßgabe der gesetzlichen Bestimmungen.

15.2 Im Übrigen haftet G&R Cybersecurity bei leichter Fahrlässigkeit nur bei der Verletzung einer wesentlichen Vertragspflicht, d.h. einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertraut und vertrauen darf (Kardinalpflicht).

15.3 In Fällen einer leicht fahrlässigen Verletzung einer wesentlichen Vertragspflicht ist die Haftung der Höhe nach beschränkt auf den bei vergleichbaren Aufträgen dieser Art typischen Schaden, der bei Beauftragung oder spätestens bei der Begehung der Pflichtverletzung vorhersehbar war, maximal jedoch auf die Höhe des Auftragswertes.

15.4 Eine weitergehende Haftung von G&R Cybersecurity vor allem darüber hinaus gehende Schadensersatzansprüche auf Ersatz von mittelbaren Schäden, Neben- und Folgeschäden, entgangenem Gewinn, Produktionsausfall etc. sind ausgeschlossen.

15.5 Für Datenverluste haftet G&R Cybersecurity nur, wenn der Auftraggeber in regelmäßigen Abständen Systemprüfungen und Datensicherungen durchgeführt hat. Die Haftung für einen eventuellen Datenverlust oder -beschädigung ist auf den Aufwand beschränkt, der bei ordnungsgemäßer Datensicherung durch den Auftraggeber erforderlich wäre, um die Daten aus dem gesicherten Datenmaterial wiederherzustellen.

15.6 Die vorstehenden Haftungsbeschränkungen gelten auch zugunsten von eventuell eingebundenen gesetzlichen Vertretern und Erfüllungsgehilfen von G&R Cybersecurity.

15.7 Ansprüche nach dem Produkthaftungsgesetz sowie Ansprüche für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit bleiben durch die vorstehenden Haftungsbeschränkungen unberührt.

16 Referenzen, Rechtswahl, Vertragssprache, Gerichtsstand

16.1 G&R Cybersecurity steht es frei, in Pressemitteilungen oder Referenzlisten die Öffentlichkeit über eine generelle Zusammenarbeit mit dem Auftraggeber und das beauftragte Projekt zu informieren, z.B. den Auftraggeber durch Auflistung als Referenzkunde auf den Webseiten zu benennen, sofern die andere Partei nicht ausdrücklich in Textform widerspricht.

16.2 Für alle Rechtsbeziehungen zwischen G&R Cybersecurity und dem Auftragnehmer gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrecht.

16.3 Vertragssprache ist deutsch.

16.4 Ausschließlicher Gerichtsstand für alle Ansprüche aus diesem Vertrag ist München, sofern der Auftraggeber Kaufmann oder einem solchen gleichgestellt, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, oder keinen Sitz oder Niederlassung in der Bundesrepublik Deutschland hat, oder nach Vertragsschluss seinen Sitz oder seine Niederlassung ins Ausland verlegt, oder der Sitz oder die Niederlassung zum Zeitpunkt der Klageerhebung nicht bekannt ist. G&R Cybersecurity ist aber auch berechtigt, am allgemeinen Gerichtsstand des Auftraggebers zu klagen.