Besondere Geschäftsbedingungen der TÜV Rheinland i-sec GmbH für Pentests

Die nachfolgenden Regelungen zum Service IT-Pentest gelten ergänzend zu den Allgemeinen Geschäftsbedingungen und den Besonderen Geschäftsbedingungen der TÜV Rheinland i-sec GmbH und gehen diesen im Fall von Widersprüchen vor.

1. Einwilligung des Auftraggebers

Der Auftraggeber erteilt seine ausdrückliche Einwilligung in alle zur Erbringung der Leistungen aus diesem Vertrag erforderlichen Maßnahmen, insbesondere zu einem etwa damit einhergehenden Zugriff auf Systeme (umfasst werden jeweils alle informationsverarbeitenden Systeme wie Soft- und Hardware sowie die darauf verarbeiteten Daten). Ferner umfasst die Einwilligung auch erforderliche Maßnahmen, die das Verschaffen, das Verändern, das Löschen oder das Abfangen von Daten, ggf. unter Überwindung einer etwaigen Zugangssicherung der vom Auftraggeber spezifizierten Systeme und/oder aus einer nichtöffentlichen Datenübermittlung und/oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage (§§ 202a ff., 303a f. StGB) betreffen.

2. Verpflichtung zur Einholung von Zustimmungen Dritter

2.1 Der Auftraggeber versichert, dass er im Vorfeld der Erbringung der Leistungen durch den TÜV Rheinland sämtliche erforderlichen Einwilligungen Dritter (insbesondere etwaiger IT-Dienstleister, Lizenzgeber, Mitarbeiter, Arbeitnehmervertretungen, Kunden oder Weitere) nachweisbar und rechtzeitig eingeholt hat oder einholen wird, oder solche nicht erforderlich sind. Diese Verpflichtung obliegt alleine dem Auftraggeber. Der TÜV Rheinland ist nicht verpflichtet, sich vom Vorliegen oder von der Vollständigkeit der Einwilligungserklärungen zu überzeugen, diese anzufragen oder diese selbst einzuholen.

2.2 Der Auftraggeber versichert, dass etwaige Dritte umfassend über die Auswirkungen und Risiken, welche mit der Leistungserbringung in mittelbaren oder unmittelbaren Zusammenhang stehen, informiert und aufgeklärt wurden. Insbesondere erfasst die Aufklärung Dritter, dass zur Erbringung der Leistung durch den TÜV Rheinland ein Zugriff auf Systeme, das Verschaffen, das Verändern, das Löschen oder das Abfangen von Daten, ggf. unter Überwindung einer etwaigen Zugangssicherung der vom Auftraggeber spezifizierten Systeme und/oder aus einer nichtöffentlichen Datenübermittlung und/oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage (§§ 202a ff., 303a f. StGB), einhergeht und ein Risiko eines möglichen ganzen oder teilweisen Datenverlustes besteht oder das mögliche Schadensausmaß bis zur technischen Irreversibilität reichen kann.

3. Eigentums-, Besitz- und Nutzungsrechte des Auftraggebers

Mit Zustandekommen des Vertrages versichert der Auftraggeber, dass er über alle notwendigen Rechte zur Durchführung der Leistungen aus diesem Vertrag auf den Zielsystemen oder den Zielapplikationen verfügt und überträgt diese für die Dauer der Leistungserbringung aus diesem Vertrag an den TÜV Rheinland. Sollten Dritte gegen den Auftragnehmer aufgrund eines Verstoßes im Sinne dieser Ziffer nach Maßgabe dieses Vertrages Ansprüche geltend machen, so wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4. Verpflichtung des Auftraggebers zur Datensicherung

4.1 Der Auftraggeber wird ausdrücklich darauf hingewiesen, dass durch die zu erbringenden Leistungen aus diesem Vertrag, Schäden oder Beeinträchtigungen an den Zielsystemen und/oder Zielapplikationen auftreten können und diese unter Umständen nur durch Wiederherstellungs-Datensicherungen oder durch teilweise umfangreiche Nachbearbeitung durch den Auftraggeber behoben werden können. Das mögliche Schadensausmaß kann bis zur technischen Irreversibilität reichen.

4.2 Der Auftraggeber verpflichtet sich, vor Beginn der technischen Durchführung eine vollumfängliche Datensicherung (Backup) sämtlicher Zielsysteme und/oder Zielapplikationen sowie den damit in Verbindung stehenden Daten durchzuführen.

4.3 Darüber hinaus verpflichtet sich der Auftraggeber sämtliche notwendigen Sicherheitsmaßnahmen, auch diejenigen, die über eine Datensicherung hinausgehen, vor Beginn der technischen Durchführung zu treffen, um die zu prüfenden Systeme und Daten notfalls nach der technischen Durchführung wieder in den ursprünglichen Zustand zurück versetzen zu können. Das Risiko eines möglichen ganzen oder teilweisen Datenverlustes, welche mittelbar oder unmittelbar aufgrund der durch den Auftragnehmer erbrachten Leistungen aus diesem Vertrag entstehen können, trägt der Auftraggeber vollumfänglich. Eine Haftung des Auftragnehmers für einen etwaigen Datenverlust, für eine Beeinträchtigung oder verursachte technische Irreversibilität der Zielsysteme und/oder Zielapplikationen im Sinne dieser Ziffer ist ausgeschlossen.

4.4 Die Verpflichtung einer vollumfänglichen Datensicherung obliegt alleine dem Auftraggeber. Der TÜV Rheinland ist nicht verpflichtet, sich von der Datensicherung zu überzeugen noch diese durchzuführen.

5. Abstimmungsverpflichtung

Spätestens im Vorgespräch benennt der Auftraggeber einen für das Projekt qualifizierten Ansprechpartner mitsamt allen notwendigen relevanten

Kontaktdaten, der jederzeit für den TÜV Rheinland verfügbar ist, um jegliche Fragen und Anforderungen in Bezug auf die Leistungserbringung und insbesondere auch tiefergehende Systemfragen zu klären, sowie Entscheidungen darüber zu treffen, wie weiter vorzugehen ist, falls es dem TÜV Rheinland gelingen sollte, in das System einzudringen.

6. Änderung des Leistungs-umfangs

6.1 Der TÜV Rheinland informiert den Auftraggeber unverzüglich über eine erkennbar notwendige Anpassung der bestellten Leistung, die einen Mehraufwand für den Auftraggeber bedeuten. Mehraufwände sind vom Auftraggeber separat zu vergüten und bedürfen einer gesonderten Beauftragung durch den Auftraggeber.

6.2 Änderungen der angebotenen Leistungen bedürfen der Schriftform.

7. Verfahren zur Änderung des Leistungsumfangs

7.1 Sofern für die Projekt-durchführung eine Änderung des Leistungsumfangs im Sinne der Ziffer 6.1 notwendig und/oder seitens des Auftraggebers gewünscht ist, vereinbaren die Parteien das nachstehende Verfahren:

7.2 Jeder Vertragspartner kann beim Projektverantwortlichen des anderen Vertragspartners in schriftlicher Form einen Änderungsantrag stellen.

7.3 Jeder Änderungsantrag enthält die Auftrags- oder Projektnummer des zugrundeliegenden Auftrages, den Namen des fachlich verantwortlichen Mitarbeiters des Auftraggebers und des TÜV Rheinland sowie eine Kurzbeschreibung der gewünschten Leistung.

7.4 Der TÜV Rheinland ist verpflichtet dem Auftraggeber mitzuteilen, ob die Prüfung eines Änderungsantrages kostenpflichtig ist. Bei kostenpflichtigen Änderungen muss der Auftraggeber dieser Prüfung des Änderungsantrages schriftlich zustimmen, bevor der TÜV Rheinland die Prüfung durchführt.

7.5 Die für eine Änderung des Leistungsumfangs erforderlichen vertraglichen Anpassungen werden in einem schriftlichen Nachtrag zu diesem Auftrag unter Verwendung des Änderungsantrages durchgeführt. Solange die Vertragspartner keine Einigung erzielen, setzt der TÜV Rheinland die Arbeiten nach dem bestehenden Vertrag, also ohne Berücksichtigung der angestrebten Änderung, fort.

8. IT- Systeme mit Bezug zum Geheimschutz

8.1 Sofern der Auftraggeber in den zu prüfenden IT-Systemen elektronische Daten verarbeitet, welche einen mittelbaren oder unmittelbaren Bezug zum staatlichen Geheimschutz oder zu anderen Rechtsvorschriften den Geheim- oder Geheimnisschutz inner- und/oder außerhalb des europäischen Wirtschaftsraums betreffend, haben (z.B. Sicherheitsüberprüfungsgesetz

des Bundes und den Schutz von Verschlusssachen SÜG, Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), Schutz von Verschlusssachen der Europäischen Union EU-VS oder Ähnliche), ist der Auftraggeber verpflichtet, den TÜV Rheinland hierauf sowie auf sämtliche für den TÜV Rheinland und für die durchzuführenden Leistungen relevanten Details schriftlich und rechtzeitig vor der Durchführung der Prüfung hinzuweisen. Falls der Auftraggeber dem TÜV Rheinland diese nicht vor der Durchführung der Prüfung mitteilt, liegt eine Pflichtverletzung des Auftraggebers vor. In diesem Falle ist der TÜV Rheinland berechtigt, vom Vertrag zurückzutreten. Bis zum Zeitpunkt des Rücktritts erbrachte Leistungen des TÜV Rheinland werden dem Auftraggeber aufwandsbezogen in Rechnung gestellt.

8.2 Dem Auftraggeber ist bewusst, dass dies dazu führen kann, dass der vom TÜV Rheinland nach eigenem Ermessen ausgewählte Prüfer (und ggf. weitere betroffene Personen) einer Sicherheitsüberprüfung nach dem SÜG oder anderen Vorschriften unterzogen werden muss. Ohne eine abgeschlossene Sicherheitsüberprüfung, die zum Ergebnis hat, dass kein Sicherheitsrisiko vorliegt, darf die betroffene Person nicht mit einer sicherheitsempfindlichen Tätigkeit betraut werden.

8.3 Der TÜV Rheinland ist in der Auswahl der Personen, die er zum Zwecke der Leistungserbringung einsetzt, frei. TÜV Rheinland hat auf die Dauer der Sicherheitsüberprüfung keinen Einfluss. Die erforderlichen Sicherheitsbescheide sind rechtzeitig durch den Auftraggeber bei der zuständigen Stelle oder Behörde zu beantragen.

8.4 Sollten Dritte gegen den TÜV Rheinland aufgrund eines Verstoßes gegen den Geheim- oder Geheimnisschutz, den der TÜV Rheinland nicht zu vertreten hat, nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den TÜV Rheinland von allen solchen Ansprüchen auf erstes Anfordern freistellen.

9. Datenschutz und Auftragsverarbeitung

9.1 Bei der Erbringung der Leistungen gemäß dem Auftrag verarbeitet der TÜV Rheinland gegebenenfalls personenbezogene Daten, die der Auftraggeber zur Erbringung der Leistungen zur Verfügung gestellt hat oder sich dem TÜV Rheinland während der Leistungserbringung offenbaren und bezüglich derer der Auftraggeber als Verantwortlicher oder als Auftragsverarbeiter im Sinne der Art. 28,29 DSGVO im datenschutzrechtlichen Sinn fungiert („Auftraggeber-Daten“).

9.2 Die folgenden Vertragsklauseln spezifizieren die Datenschutzpflichten und -rechte des Auftraggebers und des TÜV Rheinland im Zusammenhang mit der Verarbeitung der Auftraggeber-Daten zur Erbringung der Leistungen nach diesem Vertrag, insoweit und insofern eine Auftragsverarbeitung zwischen Auftraggeber und TÜV Rheinland

im Sinne der Art. 28,29 DSGVO vorliegt.

9.4 Der Auftraggeber verpflichtet sich dem TÜV Rheinland Auskunft zu erteilen, ob und inwieweit personenbezogene Daten im Sinne des Art. 4 Nr.1 DSGVO auf den Zielsystemen oder der Zielapplikation verarbeitet werden. Die Art und die Kategorien der personenbezogenen Daten werden im Rahmen eines durchzuführenden Vorgesprächs protokolliert.

10. Inhärente Risiken und Vertraulichkeit

10.1 Aufgrund der besonderen Eigenart und der typischen, inhärenten Risiken der durch den TÜV Rheinland zu erbringenden Leistungen kann der TÜV Rheinland nicht ausschließen, dass ein Datenverlust eintritt, die Funktion der Zielsysteme und/oder Zielapplikationen ganz oder teilweise, permanent oder nur zeitweilig beeinträchtigt wird oder Zugang zu vertraulichen Informationen erlangt wird, die für den TÜV Rheinland nicht zugänglich sein dürften. Der TÜV Rheinland verpflichtet sich zur Vertraulichkeit.

10.2 Diese Vertraulichkeits-verpflichtung besteht ab Vertragsbeginn und gilt nach Beendigung des Vertrages für die Dauer von fünf Jahren fort. Hinsichtlich der inhaltlichen Ausgestaltung wird auf Ziffer 9 der allgemeinen Geschäfts-bedingungen verwiesen.

11. Leistungsfristen/ -termine

11.1 Termine, die im Rahmen eines Vorgesprächs schriftlich protokolliert wurden, gelten zwischen den Parteien dann als verbindlich vereinbart, sofern der Auftraggeber das Vorgesprächsprotokoll - siehe im Einzelnen dazu auch Ziffer 13 - schriftlich bestätigt hat.

11.2 Bereits verbindlich vereinbarte Termin können nur im beiderseitigen Einverständnis verschoben oder abgesagt werden. Nur dann fallen keine Kosten für den Auftraggeber an. Das beiderseitige Einverständnis muss hierfür schriftlich festgehalten werden.

11.3 Bei einseitig durch den Auftraggeber verschobenen und/oder abgesagten verbindlich vereinbarten Terminen behält sich der TÜV Rheinland vor, folgende Kosten in Rechnung zu stellen:

- bis zu 10 Werktagen vor Testbeginn: Gebührenfrei
- zwischen 5 und 10 Werktagen vor Testbeginn: 25% des Tagessatzes
- bis zu 5 Werktagen vor Testbeginn: 100% des Tagessatzes

11.4 Gleiches gilt für Verschiebungen und/oder Absagen von verbindlich vereinbarten Terminen, die nicht durch den TÜV Rheinland zu vertreten sind.

11.5 Die Mitteilung über die Verschiebung und/oder Absage müssen schriftlich bis 18:00 Uhr werktags erfolgen, ansonsten

gelten sie erst zum nächsten Werktag.

12. Leistungsort, Leistungszeit

12.1 Die Leistung wird in Absprache mit dem Auftraggeber nach Vertragsschluss erbracht. Die Leistungszeit der technischen Durchführung der bestellten Leistungen wird im Vorgespräch mit dem Auftraggeber festgelegt und protokolliert; siehe im Einzelnen dazu auch Ziffer 13.

12.2 Der TÜV Rheinland erbringt seine Leistung gewöhnlich während seiner üblichen Geschäftszeiten, Montag bis Freitag (ME(S)Z in der Zeit von 08:00 Uhr bis 18:00 Uhr, außer an den bundesweit und in den jeweiligen Bundesländern gesetzlichen Feiertagen.

12.3 Die Leistungserbringung erfolgt, sofern nicht anders vereinbart, aus den Geschäftsräumen oder aus den Betriebsstätten des TÜV Rheinland in Form einer entfernten Leistungserbringung (Remote) unter Zuhilfenahme elektronischer Kommunikation über das Internet.

13. Vorgespräch und Protokoll

13.1 Die Einzelheiten der durchzuführenden Prüfungen und sonstigen Leistungserbringung des Vertrages, insbesondere auch die Leistungszeiträume, werden in einem gemeinsamen fernmündlichen Vorgespräch besprochen und festgelegt.

13.2 Der TÜV Rheinland wird über das Vorgespräch ein Protokoll führen und es dem Auftraggeber in elektronischer Form an den vom Auftraggeber benannten Ansprechpartner zusenden. Eine technische Durchführung der Prüfung bedarf in jedem Fall eines vom Auftraggeber schriftlich bestätigten und genehmigten Protokolls. Der Auftraggeber verpflichtet sich, das Protokoll binnen 5 Werktagen nach Erhalt gegenüber dem TÜV Rheinland schriftlich zu bestätigen. Die technische Durchführung der Prüfung kann frühestens einen Arbeitstag nach Vorliegen des vom Auftraggeber schriftlich bestätigten und genehmigten Protokolls erfolgen.

13.3 Das Protokoll wird Bestandteil des Vertrages und beinhaltet, unter anderem, die nachfolgend genannten Punkte:

- Namentliche Nennung des Protokollführers und der Teilnehmer,
- Namentliche Nennung der projektverantwortlichen Ansprechpartner sowohl des Auftraggebers als auch des TÜV Rheinland,
- Information über die festgelegte Berichtssprache und den Zeitpunkt des Versandes,
- Festlegung des Prüfungs-zeitraums mit Definition von Prüfungsbeginn und Prüfungs-ende,
- Auflistung der zu prüfenden Systeme/Services/Applikationen inklusive etwaiger Ausnahmen,
- Belehrung über die verschlüsselte Kommunikation

von als vertraulich eingestuften Informationen,
- Festlegung der Räumlichkeiten, aus denen die Durchführung der Prüfungen erfolgt,
- Information über die üblichen Zeitfenster der Durchführung der Prüfungen,
- Ggfs. Auflistung der zu prüfenden Rollen und entsprechenden Testzugängen,
- Mitwirkungspflichten des Auftraggebers,
- Information über die durch den TÜV Rheinland verwendeten IP-Adressbereiche sowie Hinweise zur Vorbereitung von durch den Auftraggeber eingesetzten Firewalls und/oder Intrusion-Prevention-Systemen,
- Belehrung über die Informationspflicht des Auftraggebers gegenüber dem TÜV Rheinland bei notwendigen Systemveränderungen oder Nichtverfügbarkeit der Systeme (Downtime) im Geltungsbereich der Prüfung während des Prüfungszeitraums,
- Sicherheits- und Risikobelehrung des Auftraggebers,
- Informationspflicht des TÜV Rheinland gegenüber dem Auftraggeber bei der Verarbeitung weiterer, im Hauptvertrag bisher nicht genannter Kategorien personenbezogener Daten
- Abstimmung des Vorgehens bei einer Übernahme eines Systems,
- Weitere.

14. Vertrags- und Projektsprache

Die Vertrags- und Projektsprache ist die deutsche Sprache. Arbeitsergebnisse in Form von Dokumentation, Berichte, Projektplänen, Präsentationen, Leit- und Richtlinien, Verfahren, Arbeitsanweisungen und Protokolle oder Ähnliches werden in deutscher Sprache erstellt. Abweichend hiervon können die Arbeitsergebnisse auf Wunsch des Auftraggebers in englischer Sprache erstellt werden, sofern dies im Protokoll des Vorgesprächs verbindlich vereinbart wurde.

15. Prüfungsart, -genauigkeit und -unschärfe

15.1 Die durchzuführende Pentest Prüfung findet in einem zeitlich festgelegten Rahmen statt und ist von ihrem Inhalt wie vereinbart begrenzt. Dabei handelt es sich lediglich um eine stichprobenartige Prüfung der Systeme des Auftraggebers zu diesem Zeitpunkt. Der Auftraggeber ist sich daher darüber im Klaren, dass das Ergebnis der Prüfung lediglich eine nicht abschließende Momentaufnahme darstellt. Unabhängig davon, ob bei der Prüfung Schwachstellen gefunden werden oder nicht, kann daher nicht gewährleistet werden, dass die geprüften Systeme (umfasst jeweils alle informationsverarbeitenden Systeme wie Soft- und Hardware sowie die darauf verarbeiteten Daten) keine oder keine weiteren Schwachstellen aufweisen, selbst wenn diese mittels der beschriebenen Prüfverfahren hätten aufgedeckt werden können.

15.2 Die Leistungen des TÜV Rheinland werden nach den allgemein anerkannten Regeln der Technik erbracht. Auch bei

optimaler Anwendung dieser Regeln ist jedoch aufgrund einer objektiven technisch-bedingten Unschärfe der eingesetzten Werkzeuge und Methoden eine zweifelsfreie Erkennung potentieller Schwachstellen nicht abschließend möglich. Die Erkennung möglicher Schwachstellen beschränkt sich auf die zum Zeitpunkt der Durchführung technischen Möglichkeiten der eingesetzten Werkzeuge. Die am Markt zur Verfügung stehenden Werkzeuge und Methoden weisen keine Erkennungsquote von 100% auf, da diese in der Regel auf dem Prinzip bereits bekannter Schwachstellen basieren.