Allgemeine Geschäftsbedingungen für PCI DSS Schwachstellen-Scans

der TÜV SÜD Sec-IT GmbH (im folgenden „Sec-IT“ genannt)

1 Allgemeines

1.1 Sec-IT stellt dem Benutzer (nachfolgend Benutzer, Auftraggeber oder Kunde genannt) mit dem Portal eine webbasierte Anwendung (nachfolgend Anwendung oder Portal genannt) zur Verfügung.

1.2 Das Portal ermöglicht einem registrierten Benutzer die Durchführung von Schwachstellen-Scans (nachfolgend Schwachstellen-Scan oder Scan genannt).

1.3 Sec-IT führt den Scan mit Hilfe der webbasierten Anwendung in automatischer Form durch. Alle Aktivitäten oder Aktionen werden durch den Benutzer veranlasst und über automatisierte Vorgänge entsprechend der Angaben des Benutzers durchgeführt.

2 Durchführung und Koordination

2.1 Die Durchführung des Schwachstellenscans erfolgt auf Veranlassung und Verantwortung des Benutzers.

2.2 Alle Aktivitäten und Aktionen werden durch den Benutzer am Portal initiiert. Der Benutzer trägt dafür Sorge, dass die initiierten Vorgänge nur für IT-Systeme durchgeführt werden, die im Besitz und/oder administrativer Hoheit des Benutzers stehen. Insbesondere darf der Benutzer keine Vorgänge initiieren, die auf IT-Systeme Dritter zielen.

2.3 Sofern der Benutzer entgegen der Vereinbarung aus Ziff. 2. 2 Vorgänge initiiert, die auf IT-Systeme Dritter zielen, stellt er Sec-IT von jeglichen Ansprüchen Dritter hieraus frei.

2.4 Sec-IT kann einen Unterauftragnehmer mit der Durchführung von Leistungen beauftragen. Für die Erbringung von PCI Leistungen beauftragt Sec-IT ausschließlich Unternehmen mit gültiger Akkreditierung als PCI Qualified Security Assessor [QSA] und Approved Scan Vendor [ASV] oder ein mit Sec-IT in Vertragsbeziehung stehendes akkreditiertes Drittunternehmen. Die in diesem Vertrag enthaltenen Bedingungen gelten in gleichem Umfang auch für einen Unterauftragnehmer.

3 Laufzeit und Kündigung

3.1 Die Vertragslaufzeit richtet sich nach den getroffenen Vereinbarungen in der Beauftragung (Auftragserteilung und/oder Leistungsbeschreibung)

3.2 Der Vertrag verlängert sich jeweils um 12 Monate, wenn er nicht mindestens drei Monate vor Ablauf der Vertragslaufzeit von einer der beiden Vertragsparteien schriftlich gekündigt wird. Darüber hinaus kann jede Vertragspartei das Vertragsverhältnis bei Vorliegen eines wichtigen Grundes außerordentlich fristlos kündigen. Sämtliche Kündigungen bedürfen der Schriftform

4 Mitwirkungspflichten

Die auf Seiten des Auftraggebers für die IT-Systeme verantwortlichen Personen müssen vom Auftraggeber im Vorfeld über die Durchführung von PCI Schwachstellen-Scans informiert werden. Der Auftraggeber ist verpflichtet, dass Sec-IT oder durch Sec-IT beauftragte Personen nicht dem Verdacht einer illegalen Hackertätigkeit ausgesetzt sind und dass die im Rahmen der Beauftragung durchgeführten Tätigkeiten zu keiner Anzeige durch den Auftraggeber führen.

Sofern erforderlich, stellt der Auftraggeber Sec-IT die für die Durchführung des Scans notwendigen Informationen im Rahmen der Payment Card Industry Data Security Standards zur Verfügung. Der Auftraggeber stellt sicher und sichert zu, dass er Kenntnis von den Anforderungen des Payment Card Industry Data Security Standards hat.

5 Preisanpassungen

5.1 Sec-IT behält sich Erhöhungen der Preise bei Vertragsverlängerung ausdrücklich vor. Sollte Sec-IT die Preise für die Leistungserbringung erhöhen wollen, so räumt sie dem Auftraggeber ein Widerspruchsrecht ein. Widerspricht der Auftraggeber der Preiserhöhung nicht innerhalb von 4 Wochen nach schriftlicher Bekanntgabe, so gilt der neue Preis ab Beginn der neuen Vertragslaufzeit.

5.2 Widersprüche müssen schriftlich an die Geschäftsadresse der Sec-IT erfolgen. Einigen sich die Parteien im Fall eines Widerspruchs nicht bis zum Ablauf der Vertragslaufzeit auf einen neuen Preis, so gelten die zuletzt vereinbarten Preise fort und der Vertrag endet automatisch zum Ende der Vertragslaufzeit, ohne dass es einer Kündigung bedarf.

6 Haftung

6.1 Sec-IT haftet für Schäden – gleich aus welchem Rechtsgrund – nur, wenn Sec-IT diese Schäden vorsätzlich oder grob fahrlässig verursacht hat oder wenn Sec-IT fahrlässig eine wesentliche Vertragspflicht („Kardinalpflicht“) verletzt hat. Sec-IT haftet im Falle der Verletzung wesentlicher Vertragspflichten stets nur für den im Zeitpunkt des Vertragsschlusses vertragstypischen, vorhersehbaren Schaden.

6.2 Soweit Sec-IT im Falle der Verletzung wesentlicher Vertragspflichten gemäß vorstehender Ziffer 5.1 für fahrlässig verursachte Schäden haftet, ist deren Ersatzpflicht jedoch der Höhe nach je Schadensfall begrenzt auf:

1.000.000,00 EUR für Sachschäden
500.000,00 EUR für Vermögensschäden.

6.3 Eine Haftung für Schäden, die durch die Verletzung nicht wesentlicher Vertragspflichten infolge einfacher Fahrlässigkeit verursacht worden sind, ist ausgeschlossen.

6.4 „Wesentliche Vertragspflichten“ sind solche Verpflichtungen, die vertragswesentliche Rechtspositionen des Auftraggebers schützen, die ihm der Vertrag nach seinem Inhalt und Zweck gerade zu gewähren hat; wesentlich sind ferner solche Vertragspflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertraut hat und vertrauen darf.

6.5 Der in Ziffern 5.1-5.3 enthaltene Haftungsausschluss bzw. die Haftungsbegrenzung gilt nicht für Schäden an Leben, Körper oder Gesundheit sowie für Ansprüche aus einer Beschaffenheitsgarantie oder nach dem Produkthaftungsgesetz.

6.6 Der Auftraggeber hat etwaige Schäden, für die Sec-IT haften soll, unverzüglich Sec-IT schriftlich anzuzeigen.

6.7 Sec-IT weist ausdrücklich darauf hin, dass durch Schwachstellen-Scans eine Beeinträchtigung des Systembetriebes oder Abstürze von Systemen des Auftraggebers möglich sind und nicht ausgeschlossen werden können. Hieraus entstehende Schäden oder Folgen sind von einer Haftung durch Sec-IT ausdrücklich ausgeschlossen. Der Auftraggeber ist verpflichtet, durch mindestens tägliche Datensicherung sicherzustellen, dass bei einem Datenverlust die Daten mit angemessenem Aufwand durch automatisierte Verfahren wieder herzustellen sind.

6.8 Sec-IT haftet auch nicht für Fehlerfreiheit, Vollständigkeit, Ablaufverfahren, zeitliche Gültigkeit oder Veränderung der Compliance Programme des Standardgebers und der darauf aufbauenden Assessment- oder Scanleistungen. Durch die Erbringung der Assessmentleistung vertritt Sec-IT nicht den Auftraggeber oder übernimmt eine Haftung (i) durch Verzögerungen oder Verluste, (ii) bei Ansprüchen Dritter, (iii) bei Nutzung und der Weiterleitung der Assessmentergebnisse basierend auf den Compliance Programmen des Standardgebers und den Ergebnissen der Assessments durch den Auftraggeber.

6.9 Soweit Schadensersatzansprüche gegen Sec-IT ausgeschlossen oder begrenzt sind, gilt dies auch für die persönliche Haftung der Organe, Sachverständigen und sonstiger Mitarbeiter sowie Erfüllungs- und Verrichtungsgehilfen von Sec-IT.

6.10 Der Auftraggeber ist verpflichtet, die üblichen Versicherungen gegen unmittelbare oder mittelbare Schäden abzuschließen.

7 Zahlungsbedingungen

7.1 Bei Jahresverträgen oder Festpreisangeboten wird der Gesamtpreis in Rechnung gestellt. Die Rechnungsstellung erfolgt nach Beauftragung durch den Auftraggeber im Voraus für die beauftragten Angebotspositionen für die Vertragsdauer von einem Jahr. Alle anderen Leistungen werden nach Erbringung der vereinbarten Leistung in Rechnung gestellt.

7.2 Entstehen bei der Leistungserbringung Verzögerungen, welche auf der Nichterfüllung von Mitwirkungspflichten durch den Auftraggeber beruhen oder verzögert sich die Leistungserbringung von Sec-IT aufgrund der Nichterfüllung von Mitwirkungspflichten durch den Auftraggeber, entsteht dem Auftraggeber kein Rückerstattungsrecht auf den Gesamtpreis. Sec-IT wird die vereinbarte Leistung unbeschadet dessen in der Folge erbringen.

7.3 Zusätzliche oder über die in der Leistungsbeschreibung definierte Anzahl von Schwachstellen-Scans hinaus durchzuführende Scans werden gesondert berechnet. Hierüber erstellt Sec-IT ein separates Angebot gegenüber dem Kunden.

7.4 Die Entgelte verstehen sich zuzüglich der gesetzlichen Umsatzsteuer in der jeweils gültigen gesetzlichen Höhe. Die Umsatzsteuer wird bei Rechnungsstellung gesondert ausgewiesen.

7.5 Beanstandungen der Rechnungen von Sec-IT sind innerhalb einer Ausschlussfrist von 14 Tagen nach Erhalt der Rechnung schriftlich begründet mitzuteilen.

8 Geheimhaltung, Nutzungsrechte, Datenschutz

8.1 Von schriftlichen Unterlagen, die Sec-IT zur Einsicht überlassen und die für die Durchführung des Auftrages von Bedeutung sind, darf Sec-IT Abschriften zu Ihren Akten nehmen.

8.2 Sec-IT behält sich an allen Bestandteilen des Portals, inklusive des Layouts sowie des gesamten Inhalts die Urheber- und sämtliche sonstigen Schutzrechte vor. Der Auftraggeber wird die Rechte von Sec-IT beachten und insbesondere keine Urheberrechtsvermerke und/oder Markenbezeichnungen und/oder sonstige Angaben in den Inhalten verändern oder beseitigen.

8.3 Sec-IT räumt dem Auftraggeber ein nicht ausschließliches und nicht übertragbares Recht zur Nutzung des Portals zur Durchführung von PCI DSS Schwachstellen-Scans ein. Weitere Rechte, insbesondere zur Nutzung des Firmennamens oder der Marke „TÜV und „TÜV SÜD“ und sonstige gewerblichen Schutzrechte werden ausdrücklich nicht eingeräumt.

8.4 Die Mitarbeiter und Sachverständigen von Sec-IT werden Geschäfts- und Betriebsverhältnisse, die bei der Ausübung der Tätigkeit zur Kenntnis gelangen, außerhalb der Durchführung des Auftrages nicht unbefugt offenbaren und verwerten.

8.5 Die Pflicht zur Geheimhaltung besteht nicht, sofern und soweit Sec-IT entsprechend den PCI-Richtlinien verpflichtet ist, Informationen zum Compliancestatus, sowie die finalen Auditreports den Kartenorganisationen oder deren beauftragten Organisationen für die abschließende Zertifizierung des Kunden zur Verfügung zu stellen.

8.6 TÜV SÜD verarbeitet und nutzt auch personenbezogene Daten ausschließlich für eigene Zwecke innerhalb der TÜV SÜD Gruppe. Die Weitergabe von Daten erfolgt nur an verbundene Gesellschaften i.S. des § 15 AktG. Dazu setzt sie auch automatische Datenverarbeitungsanlagen ein. Zur Erfüllung der Datensicherungsanforderungen der Anlage zu § 9 BDSG hat sie technisch-organisatorische Maßnahmen getroffen, die die Sicherheit der Datenbestände und der Datenverarbeitungsabläufe gewährleisten. Die mit der Verarbeitung beschäftigten Mitarbeiter sind auf das BDSG verpflichtet und gehalten, sämtliche Datenschutzbestimmungen strikt einzuhalten.

9 Gerichtsstand, Anzuwendendes Recht

9.1 Gerichtsstand für die Geltendmachung von Ansprüchen ist München.

9.2 Das Vertragsverhältnis und alle Rechtsbeziehungen hieraus unterliegen ausschließlich dem Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts des Internationalen Privatrechts (IPR) sowie des UN-Kaufrechts (CISG).

10 Zugangsdaten und Sonstiges

10.1 Der Auftraggeber ist verpflichtet etwaige Zugangsdaten zum Portal streng vertraulich aufzubewahren und Dritten nicht zugänglich zu machen. Der Auftraggeber ist verantwortlich für alle unter seinen Zugangsdaten durchgeführten Aktionen im Portal.

10.2 Soweit Sec-IT auf Webseiten Dritter verweist, übernimmt Sec-IT für die Inhalte dieser Webseiten Dritter keine Verantwortung. Sec-IT macht sich die Inhalten der Webseiten Dritter ausdrücklich nicht zu Eigen. Eine permanente Kontrolle der Webseiten Dritter ist Sec-IT nicht möglich. Die Nutzung der Verlinkungen, um auf Sec-IT -fremde Webseiten zu gelangen, geschieht mithin auf eigene Verantwortung des Auftraggebers.