WAGB-03 — Besondere Bedingungen Audit- und Pentest-Leistungen (Festpreis-/Paketverträge)

Fassung 10/2026 (verbindlich ab Veröffentlichung) · Ergänzend gelten die WAGB-01

Teil 1 — Leistungsgegenstand und Vergütung (alle Prüfleistungen)

§ 1 Vertragsgegenstand; Paket und Festpreis

1.1 werth IT erbringt Prüfleistungen (Sicherheitsaudits, Schwachstellenanalysen, Penetrationstests) auf Basis eines individuell vereinbarten Leistungspakets. Das Leistungspaket definiert mindestens: Prüfumfang (Systeme/SIDs/IP-Bereiche), Prüfart und Abschlussleistung. Mitwirkungspflichten richten sich nach § 4 WAGB-01, soweit sich aus dem Angebot nichts Abweichendes ergibt.

1.2 Die Vergütung ist ein Fest- bzw. Paketpreis. Eine Abrechnung nach Aufwand (Stunden, Tage) findet nicht statt; interne Aufwands- und Manntagsschätzungen im Angebot sind Kalkulationsgrundlage, nicht geschuldeter Leistungsumfang.

1.3 Der vereinbarte Paketpreis deckt den definierten Prüfumfang ab. Eine Erweiterung des Prüfumfangs (zusätzliche Systeme, SIDs, Prüfarten) ist nur gegen gesonderte, als Festpreis vereinbarte Zusatzpakete geschuldet.

§ 2 Leistungserfolg, Abschlussleistung

2.1 Geschuldeter Erfolg ist die Durchführung der Prüfungen im vereinbarten Umfang, die Erstellung des Prüfberichts und — soweit vereinbart — die Abschlusspräsentation gegenüber dem Kunden bzw. Besteller (zusammen „Abschlussleistung“). Die Prüfung gilt mit Lieferung der Abschlussleistung als erbracht.

2.2 Die Anzahl, Art oder der Schweregrad der festgestellten Erkenntnisse (Findings) ist nicht geschuldet. Ein Prüfungsergebnis ohne festgestellte Schwachstellen ist eine vollständige und mangelfreie Erfüllung des Vertrags.

2.3 Ein Re-Test (Nachprüfung von Behelfs- oder Abstellmaßnahmen) ist nicht geschuldet; er kann als gesondertes Paket beauftragt werden.

§ 3 Termine, Zugang, Terminvereitelung

3.1 Die Durchführung erfolgt regelmäßig remote; Ort der Leistungserbringung ist der Sitz von werth IT, soweit nicht im Auftrag etwas anderes vereinbart ist. Etwaige Reisekosten und -zeiten werden nur bei ausdrücklicher Vereinbarung nach der Preisliste berechnet.

3.2 Der Kunde stellt vereinbarte Zugänge (VPN, Test-Read-Only-Berechtigungen, Wartungsfenster) rechtzeitig und funktionsfähig bereit und benennt einen für Rückfragen und Freigaben erreichbaren Ansprechpartner, einschließlich eines Kontaktwegs für Testabbrüche (24/7, soweit produktive Systeme einbezogen sind).

3.3 Beginnt oder läuft ein vereinbartes Prüfzeitfenster und scheitert die Durchführung ganz oder teilweise aus Gründen, die der Kunde zu vertreten hat (insbesondere fehlender/fehlerhafter Zugang, nicht freigegebene Systeme, nicht erreichbarer Ansprechpartner), bleibt der Vergütungsanspruch für den betroffenen Abschnitt unberührt; es wird pauschal 50 % des auf den betroffenen Abschnitt entfallenden Paketpreises geschuldet, soweit der Kunde nicht nachweist, dass kein oder ein wesentlich geringerer Aufwand entstanden ist. Im Übrigen gilt § 642 BGB. Neuterminierungen erfolgen nach Verfügbarkeit.

3.4 Sagt der Kunde ein Prüfzeitfenster weniger als 5 Arbeitstage vorher ab oder verschiebt er es wiederholt kurzfristig, ist eine Ausfallpauschale von 50 % des anteiligen Paketpreises geschuldet; der Nachweis eines nicht oder wesentlich geringeren Schadens bleibt dem Kunden unbenommen.

3.5 Der Kunde führt vor und während der Prüfung vollständige, wiederherstellungsfähige Backups der einbezogenen Systeme; § 10.3 WAGB-01 (Haftungsbegrenzung bei Datenverlust) setzt voraus, dass dieser Pflicht nachgekommen wurde. Dem Kunden ist bekannt, dass Prüfungen Störungen oder Unterbrechungen der betroffenen Systeme verursachen können; die Grundsätze von § 9 und § 10 (Teil 2) gelten entsprechend.

§ 4 Prüfbericht und Nutzungsrechte

4.1 Der Prüfbericht enthält die Feststellungen, deren Risikobewertung nach der Methodik von werth IT und Empfehlungen zur Abstellung. Berichte werden in elektronischer Form übergeben.

4.2 Der Kunde erhält das nicht ausschließliche, nicht übertragbare Recht, den Bericht für interne Zwecke, für die Abstellung festgestellter Schwachstellen sowie gegenüber seinen Abschlussprüfern, Revision, Aufsichtsbehörden, Versicherern und Konzerngesellschaften zu nutzen und dort offenzulegen. Eine Weitergabe an Wettbewerber von werth IT oder Veröffentlichung (einschließlich Auszügen) ohne vorherige schriftliche Zustimmung von werth IT ist nicht gestattet. Die Weitergabe im Modell des § 6 WAGB-02 bzw. § 13 WAGB-02 richtet sich nach dem Vertragsverhältnis des Partners.

4.3 Der Bericht ist als Werk von werth IT anzusehen; die Urheberstellung und die Rechte an der Methodik bleiben unberührt. Der Kunde weist auf Verlangen die Urheberschaft aus.

4.4 Erkenntnisse über konkrete Schwachstellen, ihre Ausnutzungsmöglichkeiten und die zugrunde liegende Prüflogik stehen im geistigen Eigentum von werth IT (Ziffer 7.2 WAGB-01). Der Kunde erwirbt daran keine über § 4.2 hinausgehenden Rechte; eine Weitergabe einzelner Analyse-Tiefendetails an Dritte außerhalb des § 4.2 ist untersagt.

§ 5 Mängel

5.1 Mängel des Berichts (inhaltliche Unrichtigkeiten von Feststellungen, unplausible Bewertungen nach eigener Methodik) bessert werth IT innerhalb angemessener Frist kostenfrei nach. Nach Ablauf der Löschfristen der Anlage AVV (§ 7) erfolgt Nacherfüllung auf Basis der dem Kunden vorliegenden Berichtsfassung. Abweichungen in der Risikobewertung, die auf vertretbarer fachlicher Methodik beruhen, sind kein Mangel.

5.2 Im Übrigen gelten § 11 WAGB-01 und die gesetzlichen Nacherfüllungsregeln; das Rücktrittsrecht bei unerheblichen Mängeln ist ausgeschlossen (§ 323 Abs. 1 BGB entsprechend).

§ 6 Beauftragung durch Partner (Auftragskette)

6.1 Wird die Prüfleistung durch einen Partner beauftragt, ist der Partner Besteller und Vertragspartner; der Endkunde ist Empfänger der Leistung, aber nicht Vertragspartner. Der Partner ist berechtigt, den Prüfbericht an den Endkunden weiterzugeben; § 4.2 gilt für den Endkunden entsprechend.

6.2 werth IT tritt bei Durchführung und Abschlusspräsentation grundsätzlich unter eigenem Namen auf, soweit nicht ein abweichendes Auftreten (White-Label) nach § 14 WAGB-02 schriftlich vereinbart ist.

6.3 Der Partner sichert zu, die Befugnis des Endkunden zur Prüfungsgestattung (§ 4.2 WAGB-01) geprüft zu haben.

§ 7 Zahlungsziel

7.1 Die Vergütung ist mit Abschlussleistung fällig (100 % nach Abschluss), soweit der Auftrag nichts Abweichendes (z. B. Anzahlung) ausweist. § 6 WAGB-01 gilt im Übrigen.

Teil 2 — Besondere Bestimmungen für Penetrationstests und angreifende Prüfungen

§ 8 Autorisierung und Strafrecht

8.1 Der Kunde (bzw. der Partner nach § 6) versichert, Systemberechtigter im Sinne der §§ 202a, 202b, 303a, 303b StGB zu sein oder die ausdrückliche Genehmigung des Systemberechtigten zu besitzen. Die Genehmigung erstreckt sich nur auf die im Prüfplan (Rules of Engagement) benannten Systeme, Techniken und Zeitfenster.

8.2 werth IT führt Prüfungen nur auf Grundlage dieser Autorisierung durch. Der Kunde stellt werth IT von Ansprüchen Dritter frei, die aus einer fehlenden oder zu eng gefassten Autorisierung entstehen, soweit nicht die fehlende Autorisierung von werth IT zu vertreten ist.

8.3 Prüftätigkeiten auf Systemen, die über Dritte (Hosting-/SaaS-Provider) bereitgestellt werden, beschränken sich auf nicht-invasive Nachweise der Erreichbarkeit/Kommunizierbarkeit; weitergehende Angriffe unterbleiben, soweit nicht die Freigabe des Dritten schriftlich nachgewiesen ist. Die Beschaffung dieser Freigabe ist Mitwirkungspflicht des Kunden.

§ 9 Rules of Engagement (RoE)

9.1 Vor Prüfbeginn einigen sich die Parteien auf einen Prüfplan mit: Systemumfang (IP-Range, SIDs, Applikationen), erlaubten und verbotenen Prüftechniken, Zeitfenstern, Produktionsnähe und Lastgrenzen, Eskalations- und Abbruchkontakten sowie Kontakt für den Ernstfall.

9.2 Ohne ausdrückliche Einzelvereinbarung nicht gestattet: Denial-of-Service-Prüfungen, Social Engineering, physische Zugangsversuche, destruktive Lösch-/Schreibprüfungen in Produktivsystemen sowie Prüfungen außerhalb vereinbarter Zeitfenster.

9.3 Bei kritischen Störungen im geprüften Umfeld, die nachweislich auf die Prüfung zurückzuführen sind, unterbricht werth IT unverzüglich auf Anforderung des Kunden (Abbruchkontakt) und dokumentiert den Zeitpunkt.

§ 10 Verfügbarkeit und Testnebenwirkungen

10.1 werth IT minimiert Risiken für die Verfügbarkeit geprüfter Systeme nach dem Stand der Prüfdurchführung (schonende Verfahren, definierte Lastwerte, Vermeidung bekanntermaßen instabiler Prüfschritte in Produktivsystemen). Eine Garantie, dass Systeme unverändert verfügbar bleiben, ist damit nicht verbunden.

10.2 Für Schäden an Daten und Systemen durch bestimmungsgemäße, RoE-konforme Prüfung haftet werth IT nach § 10 WAGB-01. Eine Betriebshaftpflichtversicherung besteht in der zum Zeitpunkt des Auftrags gültigen Deckung.

§ 11 Kritische Feststellungen während der Prüfung

11.1 Stellt werth IT während der Prüfung eine kritische, unmittelbar ausnutzbare Schwachstelle in einem produktiven System fest, ist werth IT berechtigt, den Kunden zu informieren und die Prüfung an der betroffenen Schnittstelle vorübergehend zu unterbrechen. Eine Verpflichtung zur Information oder zur Unterbindung der weiteren Prüfung besteht nicht, soweit nicht zwingende gesetzliche Pflichten entgegenstehen; die Entscheidung liegt im pflichtgemäßen Ermessen von werth IT im Rahmen des vereinbarten Prüfumfangs.

§ 12 Responsible Disclosure und Veröffentlichung

12.1 Erkenntnisse über Schwachstellen, die nicht nur die kundeneigene Konfiguration betreffen (insbesondere Produktschwachstellen dritter Softwarehersteller), stehen im Eigentum von werth IT. werth IT ist berechtigt, solche Erkenntnisse nach Anhörung des Kunden und Einhaltung einer Embargofrist von mindestens 90 Tagen nach Erstmitteilung an den Hersteller/Kunden (kürzer nur mit Zustimmung des Kunden) an Hersteller, CERT- oder Behördenstellen zu melden oder in anonymisierter, nicht auf den Kunden zurückschließbarer Form zu veröffentlichen. Der Kunde wird über Meldungen informiert, soweit keine gesetzlichen Anzeigepflichten entgegenstehen.

12.2 Der Kunde veröffentlicht Prüfungsergebnisse nur nach Maßgabe von § 4.2.

§ 13 Datenschutz im Prüfprozess

13.1 Prüfungen können die Kenntnisnahme personenbezogener Daten (insbesondere Benutzer- und Berechtigungsdaten) einschließen. Screenshots und Anlagen werden nach Möglichkeit anonymisiert; Benutzer- und Berechtigungsangaben sind regelmäßig zwingend für die Behebbarkeit von Feststellungen und werden im Bericht aufgenommen, soweit dafür erforderlich.

13.2 Soweit hierdurch eine Auftragsverarbeitung personenbezogener Daten begründet wird, schließen die Parteien auf Verlangen die Anlage AVV (Art. 28 DSGVO) ab. Die Verantwortlichkeit des Kunden für die Daten in seinen Systemen bleibt unberührt; seine Weisungsbefugnis beschränkt sich auf die datenschutzrechtlichen Belange der Verarbeitung durch werth IT.