

## DIGITALE ZERTIFIKATE VON QUOVADIS – CERTIFICATE TERMS OF USE

Diese Certificate Terms of Use („CTU“) gelten für alle digitalen Zertifikate („Zertifikate“), unabhängig davon, ob es sich um öffentlich vertrauenswürdige TLS-/SSL-Zertifikate, Client Certificates (wie in Abschnitt 9 definiert) oder anderweitige Zertifikate handelt, die von QuoVadis, einem Unternehmen der DigiCert, Inc., an eine juristische oder natürliche Person („Kunde“) ausgestellt werden, wie im Dienstleistungsmanagement-Portal von QuoVadis und/oder der damit verbundenen API, die dem Kunden zur Verfügung gestellt wird („Portal“), oder im ausgestellten Zertifikat angegeben. Das Konto für den Zugriff und die Nutzung des Portals im Namen des Kunden wird im Folgenden als „Portalkonto“ bezeichnet. „QuoVadis“ bezeichnet die jeweilige Tochtergesellschaft von DigiCert, Inc., die die Zertifikate ausstellt, einschließlich QuoVadis Trustlink Schweiz AG, einer in der Schweiz eingetragenen Gesellschaft, QuoVadis Trustlink B.V., einer in den Niederlanden eingetragenen Gesellschaft und DigiCert Europe Belgium B.V., eine in Belgien gegründete Gesellschaft.

Durch die Annahme oder Unterzeichnung eines Vertrags, der diese Certificate Terms of Use durch Bezugnahme enthält (wobei dieser Vertrag gemeinsam mit diesen Terms of Use als „Vertrag“ bezeichnet wird), gewährleistet und bestätigt die annehmende und unterzeichnende Person (der „Unterzeichner“), dass er (i) als bevollmächtigter Vertreter des Kunden, in dessen Namen der Unterzeichner diesen Vertrag akzeptiert, handelt und ausdrücklich befugt ist, den Vertrag zu unterzeichnen und den Kunden an den Vertrag zu binden, (ii) über die Befugnis verfügt, das digitale Äquivalent eines Unternehmensstempels, -Siegels oder der Unterschrift einer Führungskraft einzuholen, um (x) die Authentizität der Website des Kunden nachzuweisen und (y) dass der Kunde für die gesamte Nutzung der Zertifikate verantwortlich ist, (iii) ausdrücklich vom Kunden bevollmächtigt wurde, Zertifikatanfragen im Auftrag des Kunden zu genehmigen, und (iv) das ausschließliche Recht des Kunden bestätigt oder bestätigen wird, die Domain(s) zu nutzen, die in die ausgestellten Zertifikate aufgenommen werden sollen.

Der Kunde und QuoVadis vereinbaren hiermit Folgendes:

### 1. Benutzer des Kontos.

Der Kunde bevollmächtigt alle Personen, die im Portalkonto als Administratoren aufgeführt werden, als Zertifikatanforderer, Zertifikatgenehmiger und Vertragsunterzeichner (wie in den EV-Richtlinien definiert) zu handeln und mit QuoVadis im Hinblick auf das Management von Zertifikaten und wichtigen Einstellungen zu kommunizieren. „EV-Richtlinien“ bezeichnet die „Extended Validation Guidelines“, die vom CA/Browser Forum („CAB-Forum“) unter [www.cabforum.org](http://www.cabforum.org) veröffentlicht werden. Der Kunde kann diese Vollmacht durch Mitteilung an QuoVadis widerrufen. Der Kunde ist dafür verantwortlich, regelmäßig zu überprüfen und zu bestätigen, welche Personen über die Vollmacht verfügen, Zertifikate anzufordern und zu genehmigen. Wenn der Kunde einen Benutzer aus dem Portalkonto entfernen möchte, unternimmt er die notwendigen Schritte, um zu verhindern, dass dieser Benutzer Zugriff auf das Portal hat, einschließlich der Änderung dessen Passworts und anderer Authentifizierungsmechanismen für dessen Portalkonto. Der Kunde ist verpflichtet, QuoVadis unverzüglich darüber zu informieren, wenn eine unberechtigte Nutzung des Portals oder des Portalkontos entdeckt wird. Der Kunde bekräftigt, dass: (i) der Kunde QuoVadis bevollmächtigt, Daten zu scannen, zu sammeln und zu erfassen, die sowohl für die Dienstleistungen von QuoVadis, und für die automatische Erneuerung von Zertifikaten und deren Upgrades relevant sind; (ii) der Kunde die Dienste ausschließlich dazu verwenden wird, um Domains, IP-Adressen oder Betriebsmittel zu scannen und zu automatisieren, die Eigentum des Kunden sind oder sich unter der Kontrolle des Kunden befinden; (iii) der Kunde die Dienste nur für den vorgesehenen Zweck und wie von QuoVadis beschrieben und vermarktet, nutzen wird.

### 2. Anfragen.

Der Kunde kann Zertifikate nur für Domainnamen anfordern, die auf den Namen des Kunden, eines verbundenen Unternehmens oder einer juristischen Person registriert sind, die QuoVadis ausdrücklich dazu bevollmächtigt, es dem Kunden zu gestatten, Zertifikate für den Domainnamen zu erhalten und zu verwalten. QuoVadis kann die Anzahl der Domainnamen, die der Kunde in ein einzelnes Zertifikat einschließen kann, nach eigenem Ermessen von QuoVadis begrenzen.

### 3. Verifikation.

Nach Erhalt eines Zertifikatantrags des Kunden prüft QuoVadis den Antrag und bemüht sich, die relevanten Informationen gemäß des Certification Practice Statement von QuoVadis sowie gemäß den geltenden Branchenstandards, Richtlinien und Anforderungen, einschließlich Gesetzen und Vorschriften, im Zusammenhang mit der Ausstellung von Zertifikaten („**Branchenstandards**“) stehen, zu überprüfen. Die Verifikation solcher Anträge unterliegt dem alleinigen Ermessen von QuoVadis, und QuoVadis kann die Ausstellung eines Zertifikats aus beliebigem Grund oder ohne Angabe von Gründen ablehnen. QuoVadis wird den Kunden benachrichtigen, wenn ein Zertifikatantrag abgelehnt wird, wobei QuoVadis nicht verpflichtet ist, eine Begründung für die Ablehnung anzugeben. „**Certification Practice Statement**“ oder „**Certificate Practice Statement**“ („**CPS**“) bezeichnet die geltenden schriftlichen Erklärungen in den Richtlinien und Praktiken, die QuoVadis für den Betrieb seiner Public Key Infrastructure („**PKI**“) heranzieht, einschließlich der jeweiligen Zeitstempelrichtlinien und -Erklärungen. Das jeweils gültige CPS von QuoVadis ist unter <https://www.quovadisglobal.com/repository> abrufbar.

#### 4. Zertifikatlebenszyklus.

Der Lebenszyklus eines ausgestellten Zertifikats ist von der Auswahl des Kunden bei der Zertifikatbestellung, den Anforderungen im CPS und dem vorgesehenen Verwendungszweck des Zertifikats abhängig. QuoVadis kann Zertifikatlebenszyklen für nicht ausgestellte Zertifikate bei Bedarf ändern, um den Anforderungen (i) des Vertrags; (ii) der Branchenstandards; (iii) der Prüfer von QuoVadis, oder (iv) eines Anbieters von Anwendungssoftware zu entsprechen. „**Anbieter von Anwendungssoftware**“ bezeichnet eine juristische Person, die Zertifikate in Verbindung mit einem bereitgestellten Root store, an dem QuoVadis beteiligt ist bzw. sich beteiligen wird, anzeigt oder verwendet. Der Kunde stimmt zu, die Nutzung eines Zertifikats und der zugehörigen Private Key (wie nachstehend definiert) nach dem Ablaufdatum des Zertifikats oder nach der vertraglich zulässigen Revozierung eines Zertifikats durch QuoVadis einzustellen.

#### 5. Ausstellung.

Ist die Verifikation eines Zertifikats zur Zufriedenheit von QuoVadis abgeschlossen, erstellt QuoVadis das angeforderte Zertifikat und übermittelt es auf geeignetem Wege an den Kunden. In der Regel übermittelt QuoVadis Zertifikate per E-Mail an eine vom Kunden angegebene Adresse, als elektronischen Download im Portal oder als Antwort auf einen API-Anruf, den der Kunde über das Portal tätigt. Öffentlich vertrauenswürdige Zertifikate werden von einem von QuoVadis ausgewählten Root- oder Intermediate Certificate ausgestellt. QuoVadis kann das zur Ausstellung von Zertifikaten verwendete Root- oder Intermediate Certificate jederzeit und ohne vorherige Benachrichtigung an den Kunden ändern. Der Kunde verpflichtet sich, bei der Bestellung und Nutzung von Zertifikaten alle geltenden Gesetze, Vorschriften und Branchenstandards einzuhalten, einschließlich der Ausfuhrkontroll- und Wirtschaftssanktionsgesetze und -Bestimmungen der Vereinigten Staaten. Der Kunde erkennt an, dass die Zertifikate nicht in Ländern oder Regionen verfügbar sind, die Einschränkungen durch das Amt zur Kontrolle von Auslandsvermögen des US-Finanzministeriums, das US-Wirtschaftsministerium, die Europäische Kommission, das Büro für die Durchsetzung finanzieller Sanktionen des britischen Finanzministeriums oder andere für QuoVadis zuständige Regierungsbehörden unterliegen.

#### 6. Zertifikatlizenz.

Mit sofortiger Wirkung nach der Übermittlung und bis das Zertifikat abläuft oder revoziert wird, ist der Kunde berechtigt, zum Vorteil der im Zertifikat genannten Person, alle ausgestellten Zertifikate und die zugehörigen Schlüsselsätze ausschließlich in Übereinstimmung mit den geltenden Gesetzen, Vorschriften, Branchenstandards sowie den in diesem Vertrag enthaltenen Bestimmungen für die im CPS genannten Zwecke einzusetzen. Alle Zertifikate, denen Anbieter von Anwendungssoftware vertrauen, unterliegen allen anwendbaren Anforderungen der Branchenstandards, einschließlich derjenigen, die in den geltenden Root store-Richtlinien des Anbieters von Anwendungssoftware und des CPS enthalten sind, unabhängig davon, wie die Zertifikate verwendet werden. Jegliche Verwendung, die nicht durch geltende Branchenstandards oder das CPS erlaubt ist, ist nicht gestattet. QuoVadis rät dringend vom Zertifikat- oder Schlüssel-Pinning, von der Verwendung von für das Web vertrauenswürdigen Zertifikaten in einer nicht-Web-PKI, oder jede andere Verwendung von Zertifikaten, die es dem Kunden erschweren würde, die Revozierungsfristen oder andere Anforderungen des CPS einzuhalten, wobei eine solche Verwendung stets nicht als ausreichender Grund für den Aufschub der Revozierung angesehen werden wird, ab. „**Schlüsselsatz**“ bezeichnet einen Satz von zwei oder mehr mathematisch zusammenhängenden Schlüsseln, als Private Key oder Key Shares nebst einem Public Key bezeichnet, wobei (i) der Public Key eine Nachricht verschlüsselt, die nur von Private Keys Schlüsseln entschlüsselt werden kann, und (ii) es rechnergestützt

unmöglich ist, die Private Keys Schlüssel herauszufinden, selbst wenn der Public Key bekannt ist. Der Kunde unterrichtet QuoVadis unverzüglich, wenn er darüber Kenntnis erlangt, dass ein Zertifikat, ein Private Key oder das Portal missbräuchlich genutzt wird. Der Kunde ist dafür verantwortlich, alle Genehmigungen und Lizenzen einzuholen und beizubehalten, die für die Bestellung, Nutzung und Bereitstellung eines Zertifikats an Endnutzer und Systeme benötigt werden, einschließlich aller gemäß den US-Exportgesetzen erforderlichen Lizenzen. SSL-Zertifikate dürfen auf einem oder mehreren physischen Servern oder Geräten gleichzeitig verwendet werden. QuoVadis ist berechtigt, eine Gebühr für die Nutzung von Zertifikaten auf zusätzlichen Servern oder Geräten zu erheben.

## 7. Schlüsselsätze.

Als „**Private Key**“ bezeichnet man den vom Kunden geheim gehaltenen Schlüssel, mit dem digitale Signaturen erstellt und/oder elektronische Aufzeichnungen oder Dateien, die mit dem zugehörigen Public Key verschlüsselt wurden, wieder entschlüsselt werden. Als „**Public Key**“ bezeichnet man den vom Kunden öffentlich bekanntgegebenen Schlüssel, der im Zertifikat des Kunden enthalten ist und mit dem geheimen Private Key des Kunden korrespondiert. Der Kunde muss (i) Schlüsselsätze mithilfe von vertrauenswürdigen Systemen erzeugen, (ii) Schlüsselsätze einsetzen, die mindestens den RSA 2048 Bit-Schlüsseln entsprechen, und (iii) alle Private Keys vertraulich behandeln. Der Kunde ist allein verantwortlich für mangelnden Schutz der Private Keys. Der Kunde gewährleistet, dass er ausschließlich Schlüsselsätze für Adobe Signing-Zertifikate und EV Code signing-Zertifikate auf einem nach FIPS 140-2, Level 2 zertifizierten Gerät erstellen und speichern wird. Alle anderen Zertifikattypen können in sicheren Hardware- oder Softwaresystemen gespeichert werden. Der Kunde ist dafür verantwortlich sicherzustellen, dass sein Erwerb, seine Nutzung oder seine Annahme von durch QuoVadis erzeugten Schlüsselsätzen gemäß diesem Vertrag unter Einhaltung der geltenden Gesetze, Verordnungen und Regeln – einschließlich, jedoch nicht beschränkt auf Gesetze, Bestimmungen und Regeln zum Import und Export – des Landes, in dem der Kunde die Schlüsselsätze erwirbt, nutzt, annimmt oder anderweitig empfängt, erfolgt. Sofern und wenn es dem Kunden gestattet ist, Private Keys (einschließlich Kopien) in Verbindung mit seiner Nutzung bestimmter QuoVadis-Dienste zu importieren oder zu exportieren, haftet QuoVadis gegenüber dem Kunden nicht für die Nutzung oder Speicherung von Private Keys (einschließlich Kopien) durch den Kunden, die nicht in dem entsprechenden Portal oder durch den entsprechenden Dienst erstellt worden sind, oder die außerhalb eines solchen Portals oder Dienstes verwendet werden, auch nachdem sie aus dem entsprechenden Portal oder Dienst exportiert wurden.

## 8. Zertifikattransparenz.

Um die ordnungsgemäße Funktion der Zertifikate während ihres Lebenszyklus zu gewährleisten, darf QuoVadis Zertifikate mit einer öffentlichen Datenbank für die Transparenz von Zertifikaten protokollieren. Protokollserverdaten sind öffentlich zugänglich. Nach ihrer Übermittlung können Daten nicht mehr aus einem Protokollserver entfernt werden.

## 9. Client Certificates.

„**Client Certificate**“ bezeichnet ein Zertifikat, das eine andere extendedKeyUsage enthält als codeSigning, Zeitstempel oder serverAuthentication. Die Verwendungszwecke für Client Certificates sind vielfältig und werden durch das Client Certificate-Profil vorgegeben. Zu den möglichen Verwendungszwecken, die im Client Certificate-Profil vorgegeben sind, zählen unter anderem die digitale Signatur, E-Mail-Verschlüsselung und kryptografische Authentifizierung. Möchte der Kunde Client Certificates beantragen, so muss er (i) die Identität und Zugehörigkeit des Antragstellers wie im CPS vorgeschrieben mittels angemessener interner Aufzeichnungen bestätigen und (ii) bestätigen, dass die bereitgestellten Daten und die mit einem Client Certificate zusammenhängenden bzw. darin enthaltenen Darstellungen in allen wesentlichen Aspekten wahr, vollständig und genau sind.

## 10. Management.

Die Ausstellung, die Verwaltung, die Erneuerung und das Revozieren eines Zertifikats durch QuoVadis erfolgt in der Regel unter Einhaltung aller über das Portal übermittelten Anweisungen des Kunden, und QuoVadis darf auf die Richtigkeit dieser Anweisungen vertrauen. Der Kunde stellt bei der Kommunikation mit QuoVadis richtige und vollständige Informationen bereit und benachrichtigt QuoVadis innerhalb von fünf Geschäftstagen, wenn sich Informationen in seinem Portalkonto ändern. Der Kunde beantwortet alle Anfragen von QuoVadis bezüglich der Gültigkeit seiner bereitgestellten Informationen innerhalb von fünf Geschäftstagen nach Eingang der Anfrage. Der Kunde prüft die Zertifikatdaten auf ihre Genauigkeit hin und verifiziert sie, bevor er das Zertifikat nutzt. Zertifikate gelten entweder dreißig (30) Tage nach der Zertifikatausstellung oder – wenn Beweise vorliegen, dass der Kunde das Zertifikat genutzt hat – mit Nutzung des Zertifikats als vom Kunden

angenommen, je nachdem, welches dieser Ereignisse früher eintritt. QuoVadis kann Ihnen zwar eine Erinnerung über den Ablauf von Zertifikaten zusenden, ist aber nicht verpflichtet, dies zu tun, und der Kunde ist allein dafür verantwortlich sicherzustellen, dass Zertifikate vor ihrem Ablauf verlängert werden. „**Geschäftstag**“ bezeichnet die Tage von Montag bis Freitag, ausgenommen gesetzliche Feiertage in dem Land, in dem der Kunde seinen Hauptsitz hat.

## 11. Registrierungsstelle.

Außer für öffentlich vertrauenswürdige TLS/SSL-Zertifikate und qualifizierte Zertifikate wird der Kunde als eine Registrierungsstelle gemäß den Bestimmungen des geltenden CPS benannt (und nimmt seine Ernennung hiermit an). Insoweit der Kunde Funktionen einer Registrierungsstelle ausübt, tut er dies unter Einhaltung des geltenden CPS, und QuoVadis kann sich auf die Handlungen des Kunden in dessen Funktion als Registrierungsstelle verlassen. Sofern sich aus dem Versäumnis des Kunden, seinen Pflichten als Registrierungsstelle strikt nachzukommen, Forderungen Dritter, Prozesse, Verfahren oder Urteile ergeben, hat der Kunde QuoVadis und dessen Geschäftsführer, leitende Angestellte, Vertreter, Mitarbeiter, Rechtsnachfolger und Abtretungsempfänger in Bezug auf alle solchen Forderungen schad- und klaglos zu halten. Wenn der Kunde als Registrierungsstelle handelt, so veranlasst er seine Abonnenten, die im Rahmen dieses Vertrags Zertifikate erhalten, die Bestimmungen der QuoVadis-Abonnentenvereinbarung unter [https://www.quovadisglobal.com/subscriber\\_agreement](https://www.quovadisglobal.com/subscriber_agreement) einzuhalten. Abonnenten des Kunden müssen die Abonnentenvereinbarung akzeptieren, bevor sie Zertifikate erhalten. Ein „**qualifiziertes Zertifikat**“ ist ein Zertifikat, das (i) gemäß den Anforderungen der entsprechend geltenden Gesetzen über Zertifizierungen und elektronische Signaturen der EU oder Schweiz ausgestellt ist, und (ii) die höchstmögliche Vertrauenswürdigkeitsstufe von „qualifiziert“ gemäß diesen Anforderungen besitzt.

## 12. Sicherheit und Nutzung von Schlüsselsätzen.

Der Kunde wird die mit einem Zertifikat verknüpften Schlüsselsätze sicher erzeugen und schützen sowie alle erforderlichen Maßnahmen ergreifen, um die Kompromittierung, den Verlust oder die unbefugte Nutzung von mit einem Zertifikat verknüpften Private Key zu verhindern. Der Kunde wird Passwörter verwenden, die den Anforderungen der Netzwerksicherheitsanforderungen des CAB-Forums und anderen relevanten Anforderungen entsprechen, um bewährte Verfahren zu erfüllen. Der Kunde gestattet seinen Mitarbeitern, Vertretern und Auftragnehmern den Zugriff auf bzw. die Nutzung von Private Keys nur dann, wenn sich der Mitarbeiter, Vertreter oder Auftragnehmer einer Überprüfung durch den Kunden (soweit gesetzlich zulässig) unterzogen hat sowie zu PKI und anderen Gebieten der Informationssicherheit geschult wurde oder entsprechende Erfahrung besitzt. Der Kunde benachrichtigt QuoVadis, fordert die Revozierung eines Zertifikats und des zugehörigen Private Key an, stellt die Nutzung des Zertifikats und des zugehörigen Private Key ein und entfernt das Zertifikat von allen Geräten, auf denen es installiert ist, wenn: (i) im Zertifikat enthaltenen Informationen falsch bzw. ungenau sind oder werden oder (ii) ein tatsächlicher oder vermuteter Missbrauch oder eine Kompromittierung des Private Key, der mit dem im Zertifikat enthaltenen Public Key verbunden ist, vorliegt. Für Code signing-Zertifikate verpflichtet sich der Kunde, die Nutzung eines Zertifikats und des zugehörigen Private Key einzustellen und unverzüglich die Revozierung des Zertifikats zu beantragen, wenn der Kunde der Auffassung ist, dass (i) im Zertifikat enthaltene Informationen falsch bzw. ungenau sind oder werden oder (ii) der Private Key, der mit dem im Zertifikat enthaltenen Public Key verbunden ist, missbräuchlich verwendet oder kompromittiert wurde, oder (c) ein Beweis vorliegt, dass das Zertifikat verwendet wurde, um verdächtigen Code zu signieren. „**Verdächtiger Code**“ bedeutet Code, der schädliche oder bösartige Funktionen jeglicher Art oder schwerwiegende Schwachstellen enthält, einschließlich Spyware, Malware und anderer Codes, die ohne Zustimmung des Nutzers installiert werden und/oder ihre eigene Löschung verhindern können, sowie Code, der auf eine Weise genutzt werden kann, die nicht von seinen Entwicklern beabsichtigt ist, um die Vertrauenswürdigkeit der Plattformen, auf denen er ausgeführt wird, zu beeinträchtigen. Der Kunde wird nicht denselben Private Key für verschiedene Zertifikatstypen verwenden. Der Kunde verwendet beispielsweise keinen Private Key, der für Codesigning verwendet wird, um ein Non-Code signing-Zertifikat anzufordern. Wenn QuoVadis erkennt, dass ein Private Key, der für einen bestimmten Zertifikatstyp oder eine bestimmte Aktion (z. B. Code signing) verwendet wurde, verwendet wird, um einen anderen Zertifikatstyp (z. B. TLS/SSL- oder Client Certificates ) anzufordern, muss QuoVadis alle Zertifikate revozieren, die mit einem solchen Private Key oder einem zugehörigen Schlüsselsatz verbunden sind und sich im zugehörigen Portalkonto des Kunden befinden oder die anderweitig von QuoVadis ausgestellt wurden. Der Kunde reagiert innerhalb von 24 Stunden auf die Anweisungen von QuoVadis in Bezug auf die Kompromittierung von Schlüsselsätzen oder den unsachgemäßen Gebrauch von Zertifikaten. Der Kunde stellt die Nutzung eines zu einem Zertifikat zugehörigen Schlüsselsatzes entweder (I) zum Zeitpunkt der Zertifikatsrevozierung oder (II) zum Ablaufdatum der zulässigen

Nutzungsperiode für den Schlüsselsatz umgehend ein, je nachdem, welches dieser Ereignisse früher eintritt. Nach der Revozierung muss der Kunde die Nutzung des Zertifikats einstellen.

### **13. Zusatzanforderungen für Schlüssel und Geräte für qualifizierte Zertifikate.**

Der Kunde wird (i) dort, wo die Verwendung eines Gerätes zur Erzeugung einer qualifizierten Signatur (QSCD) gemäß Branchenstandards vorgeschrieben ist, seine qualifizierten Zertifikate nur für die mit dem QSCD erzeugten elektronischen Signaturen auf solchen QSCD verwenden, auf denen diese qualifizierten Zertifikate gespeichert sind; (ii) wenn der Kunde eine natürliche Person ist, lediglich seinen oder ihren Private Key, der unter eigener, alleiniger Kontrolle steht, verwalten und nutzen; und (iii) wenn der Kunde eine juristische Person oder Organisation ist, lediglich ihre Private Keys, die unter eigener Kontrolle und Weisung stehen, verwalten und nutzen. Darüber hinaus bewahrt der Kunde alle Aktivierungsinformationen, die dem Kunden im Zusammenhang mit der Aktivierung des QSCD gesendet werden, getrennt von dem QSCD auf. Der Kunde muss die mit einem QSCD verbundenen Schlüsselsätze sicher schützen und alle erforderlichen Schritte unternehmen, um die Kompromittierung, den Verlust oder die unbefugte Verwendung eines mit einem QSCD verbundenen Private Key zu verhindern, einschließlich der Aufbewahrung des QSCD an einem sicheren, verschlossenen Ort, wenn dieses nicht genutzt wird.

### **14. Fehlerhafte Zertifikate.**

Der alleinige Rechtsbehelf des Kunden bei einem fehlerhaften Zertifikat („**Fehler**“) besteht darin, QuoVadis aufzufordern, nach Erhalt einer entsprechenden Mitteilung des Kunden wirtschaftlich zumutbare Anstrengungen aufzuwenden, um den Fehler zu beheben. QuoVadis ist nicht zur Behebung eines Fehlers verpflichtet, wenn der Kunde (i) das Zertifikat unsachgemäß gebraucht, beschädigt oder verändert, (ii) den Fehler nicht umgehend an QuoVadis gemeldet oder (iii) gegen eine Bestimmung des Vertrags verstoßen hat.

### **15. Gewähr für akzeptierende Dritte.**

Der Kunde erkennt an, dass die Gewähr für akzeptierende Dritte ausschließlich den akzeptierenden Dritten zugute kommt. „**Gewähr für akzeptierende Dritte**“ bezeichnet eine Gewährleistung, die einem akzeptierenden Dritten angeboten wird, der die auf der QuoVadis-Website unter <https://www.quovadisglobal.com/repository> im Vertrag für akzeptierende Dritte veröffentlichten Bedingungen erfüllt. Der Kunde besitzt keine Rechte im Rahmen dieser Gewähr für akzeptierende Dritte, einschließlich des Rechts, die Bedingungen der Gewähr für akzeptierende Dritte durchzusetzen oder im Rahmen der Gewähr für akzeptierende Dritte Forderungen zu stellen. „**Akzeptierender Dritter**“ hat die in der Gewähr für akzeptierende Dritte festgeschriebene Bedeutung. Ein Anbieter von Anwendungssoftware ist kein akzeptierender Dritter, wenn die von ihm vertriebene Anwendungssoftware lediglich Angaben zu einem Zertifikat anzeigt oder die Nutzung des Zertifikats bzw. der digitalen Signatur ermöglicht.

### **16. Zusicherungen.**

Für jedes angeforderte Zertifikat gewährleistet der Kunde und sichert zu, dass:

- a. er das Nutzungsrecht für (i) die im Zertifikat genannten Domain-Namen und (ii) die im Zertifikat genannten gebräuchlichen Bezeichnungen und Namen einer Organisation besitzt oder deren rechtmäßiger Eigentümer ist;
- b. er das Zertifikat nur für autorisierte und rechtmäßige Zwecke nutzen wird, insbesondere wird er das Zertifikat nicht nutzen, um verdächtigen Code zu unterzeichnen, und das Zertifikat und den Private Key ausschließlich in Einklang mit dem Zweck des Zertifikats, des CPS, allen anwendbaren Zertifikatrichtlinien und des Vertrags nutzen wird;
- c. er das CPS gelesen und verstanden hat und es akzeptiert;
- d. er QuoVadis umgehend schriftlich über jegliche Nichteinhaltung des CPS oder der Grundanforderungen informieren wird; und
- e. die im Zertifikat genannte Organisation und der registrierten Inhaber des Domain-Namens die jeweiligen Zertifikatanforderungen kennt und sie genehmigt.

## 17. Einschränkungen.

Der Kunde nutzt ein TLS/SSL-Zertifikat lediglich auf den Servern, die unter den im ausgestellten Zertifikat aufgeführten Domain-Namen zugänglich sind. Darüber hinaus erklärt der Kunde, Folgendes zu unterlassen:

- a. Änderungen, Unterlizenzierungen oder Erstellung von abgeleiteten Werken der TLS/SSL-Zertifikate (es sei denn, dies ist erforderlich, um das Zertifikat für den angegebenen Zweck zu nutzen) oder Private Keys;
- b. Hochladen oder Verteilen von Dateien oder Software, die den Betrieb eines anderen Computers stören können;
- c. macht Zusicherungen über oder nutzt ein TLS/SSL-Zertifikat für einen anderen Zweck als gemäß CPS erlaubt;
- d. seine Zugehörigkeit zu einer anderen juristischen Person vorzutäuschen oder falsch darzustellen;
- e. ein Zertifikat oder eine zugehörige Software bzw. einen zugehörigen Dienst (z. B. das Portal) auf eine Art und Weise zu verwenden, die anzunehmender Weise zu zivil- oder strafrechtlichen Schritten gegen den Kunden oder QuoVadis führen kann;
- f. ein Zertifikat oder eine damit verbundene Software zu nutzen, um das Vertrauen eines Dritten zu verletzen oder um unaufgefordert Massennachrichten zu senden oder zu empfangen;
- g. Code signing-Zertifikate zu verwenden, um verdächtigen Code zu signieren;
- h. ein Code signing-Zertifikat zu beantragen, wenn es sich beim Public Key im Zertifikat um ein Non-Code signing-Zertifikat handelt oder wenn der Public Key mit einem Non-Code signing-Zertifikat genutzt wird oder werden wird;
- i. die einwandfreie Funktionsfähigkeit der Website von QuoVadis oder jegliche Transaktionen, die über die Website von QuoVadis durchgeführt werden, zu beeinträchtigen;
- j. zu versuchen, ein Zertifikat zu nutzen, um andere Zertifikate auszustellen;
- k. die technische Implementierung der Systeme oder Software von QuoVadis zu überwachen, zu beeinträchtigen oder durch Reverse-Engineering rückzuentwickeln oder auf andere Weise wissentlich die Sicherheit der Systeme oder Software von QuoVadis zu gefährden;
- l. Zertifikatinformationen an QuoVadis zu übermitteln, die geistige Eigentumsrechte eines Dritten verletzen; oder
- m. vorsätzlich einen Private Key zu erstellen, der dem Private Key von QuoVadis oder eines Dritten substantiell ähnlich ist.

## 18. Zertifikatsrevozierung (Certificate Revocation).

QuoVadis kann ein Zertifikat aus den im CPS genannten Gründen revozieren, unter anderem wenn QuoVadis aus berechtigten Gründen der Auffassung ist, dass:

- a. der Kunde die Revozierung des Zertifikats beantragt hat oder die Ausstellung des Zertifikats nicht genehmigt hat;
- b. der Kunde gegen den Vertrag oder eine Verpflichtung, die er gemäß des CPS hat, verstoßen hat;
- c. eine Bestimmung eines Vertrags mit dem Kunden, die eine Zusicherung oder Verpflichtung im Zusammenhang mit der Ausstellung, Nutzung, Verwaltung oder der Revozierung des Zertifikats enthält, endet oder für ungültig erklärt wird;
- d. der Kunde auf eine Liste mit von einer Regierung verbotenen natürlichen oder juristischen Personen gesetzt wird oder seine Geschäfte von einem gemäß den Gesetzen der Vereinigten Staaten verbotenen Standort aus tätigt;
- e. das Zertifikat falsche oder irreführende Informationen enthält;
- f. das Zertifikat ohne Genehmigung, nicht für den vorgesehenen Zweck oder zum Signieren von verdächtigem Code verwendet wurde;

- g. der mit dem Zertifikat verbundene Private Key offengelegt oder kompromittiert wurde;
- h. das Zertifikat (i) missbräuchlich verwendet wurde, (ii) unter Verletzung von Gesetzen, des CPS oder den Branchenstandards verwendet wurde oder (iii) direkt oder indirekt für rechtswidrige oder betrügerische Zwecke, wie Phishing-Angriffe, Betrug oder zur Verbreitung von Malware oder zu anderen rechtswidrigen oder betrügerischen Zwecken verwendet wurde;
- i. die Zertifikatsrevozierung gemäß den Branchenstandards oder des CPS von QuoVadis erforderlich ist oder um Rechte, vertrauliche Informationen, Betriebsabläufe oder den Ruf von QuoVadis oder eines Dritten zu schützen.

## 19. Weitergabe von Informationen.

Der Kunde erkennt an und stimmt zu, dass, wenn (i) das Zertifikat oder der Kunde als Quelle von verdächtigem Code identifiziert wird, (ii) die Berechtigung zur Beantragung des Zertifikats nicht überprüft werden kann oder (iii) das Zertifikat aus anderen Gründen als auf Antrag des Kunden revoziert wird (z. B. aufgrund des Kompromittierens eines Private Key, der Erkennung von Malware etc.), QuoVadis berechtigt ist, Informationen über den Kunden, über Anwendungen oder Objekte, die mit dem Zertifikat signiert wurden, über das Zertifikat und die Begleitumstände an andere Zertifizierungsstellen oder Branchengruppen, einschließlich des CAB-Forums, weiterzugeben.

## 20. Branchenstandards.

Beide Parteien verpflichten sich zur Einhaltung aller Branchenstandards und Gesetze, die für die Zertifikate gelten. Wenn sich ein geltendes Gesetz oder der Branchenstandard ändert und diese Änderung die Zertifikate oder andere nach diesem Vertrag bereitgestellte Dienstleistungen betrifft, kann QuoVadis die Dienstleistungen modifizieren oder den Vertrag ändern oder kündigen, sofern dies notwendig ist, um der Änderung nachzukommen.

## 21. Ausrüstung.

Der Kunde ist auf eigene Kosten verantwortlich für (i) jegliche Computer, Telekommunikationsausrüstung, Software, Internetzugang und Kommunikationsnetzwerke, die (gegebenenfalls) erforderlich sind, um die Zertifikate und die damit verbundene Software und Dienstleistungen von QuoVadis zu nutzen; und (ii) das Verhalten des Kunden, die Wartung, den Betrieb und die Entwicklung seiner Website sowie für dessen Inhalte.

## 22. Zertifikatbegünstigte.

Akzeptierende Dritte und Anbieter von Anwendungssoftware sind ausdrücklich Drittbegünstigte der Verpflichtungen und Zusicherungen des Kunden im Zusammenhang mit der Nutzung und Ausstellung eines Zertifikats. Die akzeptierenden Dritten und Anbieter von Anwendungssoftware sind keine ausdrücklichen Drittbegünstigten im Hinblick auf die Software von QuoVadis.

## 23. Intermediate Certificates.

Dieser Abschnitt 233 gilt nur, wenn der Kunde ein dediziertes privates Root Certificate und/oder ein Intermediate Certificate für die Ausstellung von privaten Zertifikaten oder öffentlich vertrauenswürdigen Zertifikaten, wie in einem Bestellformular angegeben, über ein Bestellformular kauft.

- a. Erstellung. Innerhalb von 60 Tagen nach Erhalt der entsprechenden Zahlung gemäß dem Vertrag sowie nach Erhalt der von QuoVadis benötigten Informationen, um das Root Certificate und/oder Intermediate Certificate gemäß Unterabsatz b. zu erstellen, erstellt QuoVadis ein Root Certificate und/oder ein Intermediate Certificate für die (i) Ausstellung von nicht öffentlich vertrauenswürdigen Zertifikaten über das Portal oder (ii) öffentlich vertrauenswürdigen Zertifikaten, wie in einem Bestellformular angegeben. Ein „**privates Zertifikat**“ bedeutet ein Zertifikat, das nicht in einen Trust Store eingebettet ist. Ein „**Root Certificate**“ bedeutet ein selbstsigniertes Zertifikat, das in einem sicheren Offline-Status gespeichert und verwendet wird, um andere Zertifikate auszustellen. „**Intermediate Certificate**“ bedeutet ein Zertifikat, das von einem privaten Schlüssel signiert wird, der zu einem Root Certificate gehört und verwendet wird, um Zertifikate für die Nutzung durch den Kunden auszustellen.

- b. Inhalte. QuoVadis und der Kunde arbeiten in gutem Glauben zusammen, um die angemessenen Inhalte des Root Certificate und/oder des Intermediate Certificate festzulegen. Der Kunde muss QuoVadis alle von QuoVadis für die Erstellung des Root Certificate und/oder Intermediate Certificate erforderlichen Informationen innerhalb von zwölf (12) Monaten nach Abschluss eines Vertrags über die Erstellung dieses Root Certificate und/oder Intermediate Certificate zur Verfügung stellen. Wenn der Kunde nicht alle erforderlichen Informationen innerhalb dieses Zeitraums bereitstellt, verwirkt der Kunde das Recht, das Root Certificate und/oder das Intermediate Certificate anzufordern, und QuoVadis behält alle für die Erstellung des Root Certificate und/oder Intermediate Certificate gezahlten Gebühren ein. Nachdem ein Intermediate Certificate erstellt wurde, kann der Kunde die Inhalte dieses Intermediate Certificate nicht mehr ändern, er kann jedoch so viele Kopien des Intermediate Certificate erstellen, wie benötigt werden. Intermediate Certificates haben einen festgelegten Lebenszyklus von zehn Jahren, nachdem sie ohne Verlängerung ablaufen. Der Kunde ist dafür verantwortlich sicherzustellen, dass alle von einem Intermediate Certificate ausgestellten Zertifikate mindestens zwei Jahre vor Ablauf des Intermediate Certificate ablaufen. QuoVadis hat das Recht, die aus den Intermediate Certificates ausgestellten Zertifikate, die während der zwei Jahre vor Ablauf des Intermediate Certificate noch gültig sind, zu revozieren.
- c. Eigentum. QuoVadis behält das Alleineigentum am Intermediate Certificate, wird jedoch, sofern hierin nichts anderes festgelegt ist, das Intermediate Certificate nur in Übereinstimmung mit den Anweisungen verwenden, die der Kunde über das Portal bereitstellt. Der Kunde kann Kopien des Intermediate Certificate erstellen und diese Kopien des Intermediate Certificate an seine eigenen Endnutzer und Kunden vertreiben.
- d. Hosting. QuoVadis verpflichtet sich, den Private Key des Intermediate Certificate in sicheren PKI-Systemen von QuoVadis zu hosten. Unter keinen Umständen ist der Kunde berechtigt, den Private Key des Intermediate Certificate von den PKI-Systemen von QuoVadis zu entfernen oder von einem Dritten entfernen zu lassen. QuoVadis stellt dem Kunden CRL-/OCSP-Dienste zur Verfügung und hostet diese für den Kunden. QuoVadis stellt die CRL/OCSP-Dienste nach Beendigung des Vertrags weiterhin zur Verfügung, bis alle gemäß diesem Vertrag ausgestellten Zertifikate abgelaufen sind oder revoziert wurden. Für ein Intermediate Certificate, das öffentlich vertrauenswürdige Zertifikate ausstellt, wird das Intermediate Certificate durch das WebTrust-Audit von QuoVadis abgedeckt, weil das Intermediate Certificate öffentlich vertrauenswürdige Zertifikate ausstellt, in der PKI von QuoVadis gehostet und von den Mitarbeitern von QuoVadis verwaltet wird. Wenn sich Branchenstandards oder die Richtlinien eines Anbieters von Anwendungssoftware in einer Weise ändern, die eine separate Prüfung des Intermediate Certificate erfordert, werden QuoVadis und der Kunde nach Treu und Glauben zusammenarbeiten, um die erforderliche Prüfung zu erlangen.
- e. Revoizierung. QuoVadis hat das Recht, das Intermediate Certificate zu revozieren, wenn (i) der Kunde die Revoizierung schriftlich bei QuoVadis beantragt und dabei eine bestimmte Verletzung eines Branchenstandards anführt; (ii) QuoVadis aus berechtigten Gründen der Auffassung ist, dass das Intermediate Certificate kompromittiert wurde; (iii) der Kunde wesentlich gegen den Vertrag verstößt und es versäumt, innerhalb von 30 Tagen nach Benachrichtigung über die Vertragsverletzung, Abhilfe zu schaffen; (iv) der Kunde das Intermediate Certificate weiterhin nutzt, nachdem das Recht des Kunden auf Nutzung des Intermediate Certificate beendet wurde, oder (v) wenn QuoVadis vernünftigerweise davon ausgeht, dass die Revoizierung nach Branchenstandards erforderlich ist.
- f. Einschränkungen. Der Kunde verpflichtet sich, Folgendes zu unterlassen: (i) zusätzliche Intermediate Certificates mithilfe des Intermediate Certificate zu erstellen oder versuchen zu erstellen; (ii) das Intermediate Certificate an einen Dritten zu verkaufen, zu vertreiben, zu vermieten, zu verleasen, zu lizenzieren, abzutreten oder anderweitig an einen Dritten zu übertragen; (iii) ein von QuoVadis zur Verfügung gestelltes Intermediate Certificate nach dessen Ablauf, Revoizierung oder nach Beendigung dieses Vertrags zu nutzen; (iv) ein von QuoVadis zur Verfügung gestelltes Intermediate Certificate zu verändern, zu bearbeiten oder zu überarbeiten; oder (v) das Intermediate Certificate zu nutzen, wenn der Kunde Grund zu der Annahme hat, dass der Private Key des Intermediate Certificate kompromittiert wurde.

## 24. EULA und Nutzungsbedingungen für Dritte.

- a. Die Nutzung einer QuoVadis Dienstleistung (oder einer Komponente davon) in Form von Software („**lizenzierte Software**“) durch den Kunden, die auf Ausrüstung oder Geräten durch oder im Auftrag des Kunden installiert werden soll, wird durch den Lizenzvertrag geregelt, der die lizenzierte Software begleitet; sollte die lizenzierte Software nicht



von einem Lizenzvertrag begleitet werden, wird die Nutzung dieser lizenzierten Software durch den Endnutzerlizenzvertrag für Software (End User License Agreement – „EULA“) geregelt, der unter <http://www.digicert.com/eula> verfügbar ist. Für die Zwecke der Certificate Terms of Use gelten alle Bezugnahmen im EULA auf DigiCert als Bezugnahmen auf QuoVadis.

- b. Der Kunde erkennt an und stimmt zu, dass wenn das Zertifikat des Kunden eine Rechtsträger-Kennung (Legal Entity Identifier – „LEI“) enthält, die von Ubisecure Oy zur Verfügung gestellt wird, für die LEI des Kunden und für die Nutzung des RapidLEI Legal Entity Identifier Management System oder eine nachfolgende Dienstleistung die Ubisecure Oy – RapidLEI-Nutzungsbedingungen gelten, die unter <https://rapidlei.com/documents/global-lei-system-terms/> verfügbar sind.
- c. Der Kunde bestätigt und stimmt zu, dass die Nutzung von QuoVadis PQC-Toolkit (Post-Quantum Cryptographic Toolkit, das „PQC-Toolkit“) zusätzlich zu den Bedingungen sonstiger geltender Lizenzvereinbarungen den folgenden Bedingungen unterliegt: (i) die dem Kunden in Bezug auf das PQC-Toolkit gewährte Lizenz ist eine nicht exklusive, kündbare Lizenz, die nur in Verbindung mit einem QuoVadis-Zertifikat verwendet werden darf, das eine Unterschrift und einen Public Key beinhaltet, die von oder mithilfe des PQC-Toolkits oder damit in Verbindung stehenden Test- und Konfigurationsaktivitäten erzeugt wurden; (ii) der Kunde erwirbt kein geistiges Eigentum oder sonstige Schutzrechte am PQC-Toolkit oder an damit verbundenem geistigen Eigentum; (iii) der Kunde wird das PQC-Toolkit weder rückentwickeln noch übersetzen, disassemblieren, dekompileieren, entschlüsseln oder zerlegen; (iv) der Kunde wird die Nutzung des PQC-Toolkits nach Kündigung der diesbezüglichen Dienste von QuoVadis einstellen; (v) die ISARA Corporation ist dem Kunden gegenüber nicht für etwaige Schäden, gleich welcher Art, haftbar; (vi) der Kunde wird das PQC-Toolkit nur gemäß den geltenden Gesetzen des Landes oder Gebietes importieren, exportieren oder wiederverwenden, in denen das PQC-Toolkit genutzt wird oder aus dem oder in das es importiert, exportiert oder re-exportiert wird; (vii) QuoVadis übernimmt keine Gewährleistung, weder ausdrücklich noch stillschweigend, in Bezug auf das PQC-Toolkit im Namen der ISARA Corporation und (viii) der Kunde wird keine Hinweise auf Urheberrecht, Marken oder Patente verändern, die im PQC-Toolkit oder in damit verbundenen Materialien enthalten oder beigefügt sind.
- d. Wenn der Kunde Produkte oder Dienstleistungen von Thales, Gemalto oder SafeNet von DigiCert erwirbt, unterliegt die Nutzung dieser Produkte oder Dienstleistungen durch den Kunden der Thales-Endbenutzer-Lizenzvereinbarung, die unter <https://cpl.thalesgroup.com/legal> verfügbar ist, und der Kauf von Thales Cloud-basierten Diensten via DigiCert unterliegen den Bedingungen, die unter <https://www6.thalesgroup.com/service-specific-terms> verfügbar sind.

**25. Flow-Down-Anforderungen.** Der Kunde ist nicht berechtigt, die technische Implementierung der Systeme oder Software von QuoVadis zu überwachen, zu beeinträchtigen oder durch Reverse Engineering rückzuentwickeln oder auf andere Weise wissentlich zu kompromittieren, und muss seinen benannten Herstellern, sofern vorhanden, dieselben Einschränkungen auferlegen.

## **26. Von Microsoft geforderte zusätzliche Verpflichtungen.**

- a. Wenn der Kunde die Microsoft Auto Enrollment-Komponente nutzt, gelten die folgenden von MICROSOFT GEFORDERTEN ZUSÄTZLICHEN VERPFLICHTUNGEN:
- b. Gewährleistungsausschluss. MICROSOFT UND SEINE VERBUNDENEN UNTERNEHMEN ÜBERNEHMEN KEINE AUSDRÜCKLICHEN, STILLSCHWEIGENDEN ODER GESETZLICHEN GEWÄHRLEISTUNGEN IM HINBLICK AUF DIE GEMÄSS DIESEM VERTRAG BEREITGESTELLTE SERVER-SOFTWARE („SERVER-SOFTWARE“), UND ÜBERNEHMEN KEINE VERANTWORTUNG FÜR DEREN LEISTUNG ODER LEISTUNGSUNFÄHIGKEIT. LAUT MICROSOFT WIRD DIE SERVER-SOFTWARE „WIE BESEHEN“ UND MIT MÖGLICHEN FEHLERN BEREITGESTELLT, UND MICROSOFT UND SEINE VERBUNDENEN UNTERNEHMEN LEHNEN HIERMIT ALLE ANDEREN GEWÄHRLEISTUNGEN, PFLICHTEN UND BEDINGUNGEN, SOWOHL AUSDRÜCKLICH ALS AUCH STILLSCHWEIGEND ODER GESETZLICH, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF, JEDLICHE STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN, BEDINGUNGEN FÜR MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, ZUVERLÄSSIGKEIT ODER VERFÜGBARKEIT (FALLS VORHANDEN) IM HINBLICK AUF DIE SERVER-SOFTWARE AB. DARÜBER HINAUS ÜBERNEHMEN MICROSOFT UND SEINE VERBUNDENEN UNTERNEHMEN KEINE GEWÄHRLEISTUNG ODER GEWÄHR FÜR RECHTSMÄNGEL FÜR DIE

UNGESTÖRTE NUTZUNG, DIE ÜBEREINSTIMMUNG MIT DER BESCHREIBUNG ODER NICHTVERLETZUNG VON RECHTEN IM HINBLICK AUF DIE SERVER-SOFTWARE.

- c. Ausschluss bestimmter Schadenersatzansprüche. IN NACH GELTENDEM RECHT MAXIMAL ZULÄSSIGEN UMFANG HAFTET MICROSOFT IN KEINEM FALL FÜR JEDLICHE BESONDERE SCHÄDEN, ZUFÄLLIGEN SCHÄDEN, PÖNALEN, INDIRECTE SCHÄDEN ODER FOLGESCHÄDEN, (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF, SCHÄDEN AUS ENTGANGENEM GEWINN ODER DEM VERLUST VON VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, WEGEN BETRIEBSUNTERBRECHUNGEN, FÜR PERSONENSCHÄDEN, FÜR DEN VERLUST DER PRIVATSPHÄRE, FÜR DIE NICHTERFÜLLUNG EINER PFLICHT, EINSCHLIESSLICH NACH TREU UND GLAUBEN ODER UNTER ANGEMESSENER SORGFALT, FÜR FAHRLÄSSIGKEIT UND FÜR JEDEN ANDEREN FINANZIELLEN ODER SONSTIGEN VERLUST), DIE SICH AUS DER NUTZUNG ODER IN IRGENDWEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SERVER-SOFTWARE ERGEBEN, DER BEREITSTELLUNG ODER NICHTBEREITSTELLUNG VON SUPPORT ODER ANDEREN DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND DAMIT ZUSAMMENHÄNGENDEN INHALTEN DURCH DIE SERVER-SOFTWARE ODER ANDERWEITIG, DIE SICH AUS DER NUTZUNG DER SERVER-SOFTWARE ODER ANDERWEITIG UNTER ODER IN VERBINDUNG MIT EINER DIESER BEDINGUNGEN DER DIENSTLEISTUNGSBESCHREIBUNGEN ERGEBEN, AUCH IM FEHLERFALL, EINER UNERLAUBTEN HANDLUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT), EINER GEFÄHRDUNGSHAFTUNG, EINER VERTRAGSVERLETZUNG ODER EINER VERLETZUNG DER GARANTIE VON MICROSOFT, UND SELBST WENN MICROSOFT ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.
- d. Anforderungen an die Server-Software. Der Kunde darf nur eine (1) Kopie (es sei denn, in der entsprechenden Bestellung wird etwas anderes angegeben) der gemäß diesem Vertrag bereitgestellten Server-Software erstellen, wie in der Begleitdokumentation der Software angegeben, und zwar nur, um mit nativen Microsoft Windows 2000 Professional, Windows XP Home oder Professional, oder Vista Client-Betriebssystemen (bzw. deren Nachfolgesystemen) zu interagieren oder zu kommunizieren. Der Kunde darf die Server-Software unter keinen Umständen auf einem Personal Computer verwenden. Für die Zwecke des Vorstehenden bezeichnet ein „**Personal Computer**“ jeden Computer, der so konfiguriert wurde, dass sein Hauptzweck die Nutzung durch jeweils eine Person ist, und der ein Video-Display und eine Tastatur verwendet.
- e. Drittbegünstigte. Ungeachtet jeglicher widersprüchlicher Bestimmungen in diesem Vertrag stimmt der Kunde hiermit zu, dass die Microsoft Corporation als Lizenzgeber von in die Server-Software integriertem geistigen Eigentum ein Drittbegünstigter der Bedingungen dieses Abschnitts 266 sein soll, mit dem Recht, hierin enthaltene Bestimmungen durchzusetzen, die integriertes geistiges Eigentum von Microsoft oder andere Interessen von Microsoft betreffen, die mit den Bedingungen dieses Vertrags verbunden sind.
- f. Server-Klasse 2. Wenn der Kunde die Server-Klasse 2 gewählt hat, kann der Kunde die Server-Software auf einem Server nutzen, der (a) nicht mehr als vier (4) Prozessoren enthält, von denen jeder Prozessor über maximal zweiunddreißig (32) Bits und vier (4) Gigabyte RAM verfügt, und (b) nicht in der Lage ist, Speicher hinzuzufügen, zu ändern oder zu entfernen, ohne dass der Server, auf dem sie läuft, neugestartet wird („**Hot-Swapping-Fähigkeiten**“). Der Kunde ist nicht berechtigt, die Server-Software im Zusammenhang mit jeglicher Software zu nutzen, die Hot-Swapping- oder Clustering-Fähigkeiten unterstützt, wobei „**Clustering-Fähigkeiten**“ die Fähigkeit bezeichnet, einer Gruppe von Servern die Funktion einer einzigen Hochverfügbarkeitsplattform (High-Availability-Plattform) für den Betrieb von Anwendungen unter Verwendung von Anwendungs-Failover zwischen Serverknoten in der Gruppe zu ermöglichen.
- g. Prüfrechte. Sofern der Kunde mindestens vierzehn (14) Tage im Voraus darüber informiert wurde, ist QuoVadis berechtigt, beim Kunden Prüfungen durchzuführen und die Räumlichkeiten und Verfahren des Kunden während der regulären Geschäftszeiten zu inspizieren, um zu überprüfen, ob der Kunde alle Vertragsbedingungen einhält. Ungeachtet gegenteiliger Bestimmungen in diesem Vertrag (einschließlich und ohne Einschränkung aller Vertraulichkeitsbestimmungen) gilt, dass, wenn der Kunde sich einer solchen Prüfung nicht unterzieht, QuoVadis Grund zu der Annahme hat, dass der Kunde möglicherweise die Bedingungen der Dienstleistungsbeschreibungen nicht einhält; in diesem Fall stimmt der Kunde zu, dass QuoVadis (i) die Identität des Kunden gegenüber akzeptierenden Dritten und Anbietern von Anwendungssoftware offenlegen kann und (ii) dass QuoVadis die Grundlage für die Annahme der Nichteinhaltung offenlegen darf.

- h. Multiplexing-Geräte. Hardware oder Software, durch die die Anzahl der Nutzer reduziert wird, die direkt auf die von der Server-Software bereitgestellten Dienstleistungen zugreifen oder diese nutzen, reduziert nicht die Anzahl der Nutzer, die als auf die von der Server-Software bereitgestellten Dienstleistungen zugreifen oder diese nutzen erachtet werden. Die Anzahl der Nutzer, die auf die Server-Software zugreifen oder diese nutzen, entspricht der Anzahl der Nutzer, die entweder direkt oder über ein Multiplexing-Gerät auf Dienstleistungen zugreifen oder diese nutzen, die entweder (a) von der Server-Software oder (b) jeder anderen Software oder jedem anderen System, bei dem die Authentifizierung oder Autorisierung für diese Software oder dieses System durch die Server-Software erfolgt (ein „**anderes authentifiziertes System**“) bereitgestellt wird. In diesem Vertrag bezeichnet ein „**Multiplexing-Gerät**“ jede Hardware oder Software, die über eine reduzierte Anzahl von Verbindungen direkt oder indirekt Zugriff auf Dienstleistungen gewährt oder erhält, die von der Server-Software oder jedem anderen authentifizierten System für oder im Auftrag mehrerer anderer Nutzer bereitgestellt werden.
- i. Windows-CAL-Anforderung. Der Kunde muss für jeden Nutzer, der auf die von der Server-Software oder einem anderen authentifizierten System bereitgestellten Dienstleistungen zugreift oder diese entweder direkt oder über ein Multiplexing-Gerät oder von einem solchen Gerät aus nutzt, eine separate Windows-CAL erwerben und zuordnen. Eine „**Windows-CAL**“ bedeutet (a) eine Windows Device Client Access License („**CAL**“), oder eine Windows User CAL, in beiden Fällen für ein Server-Betriebssystemprodukt „Microsoft Windows Server 2003“ (Standard-Edition, Enterprise-Edition oder Datacenter-Edition) (oder ein Nachfolgeprodukt) („**Windows-Server**“); oder (b) eine Microsoft Core CAL, die einer einzelnen Person oder einem elektronischen Gerät das Recht einräumt, auf Windows-Server zuzugreifen und diese zu nutzen, entweder im Fall (a) oder (b), die der Kunde zur Verwendung mit einem oder mehreren dieser Microsoft Windows Server-Betriebssystemprodukte oder elektronischen Geräten erworben hat, und die auf einer „pro Benutzer“-Grundlage oder „pro Gerät“-Grundlage verwendet werden.

## 27. Von Adobe geforderte Zusatzverpflichtung

Falls dem Kunden Signaturzertifikate von Adobe ausgestellt werden, verpflichtet sich der Kunde zur:

- a. Einhaltung der AATL Zertifikatsrichtlinie 2.0 der Adobe Systems Inc., die derzeit unter [https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/\\_jcr\\_content/main-pars/download-section/download-1/aatl\\_technical\\_requirements\\_v2.0.pdf](https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf) zum Download zur Verfügung steht und insbesondere, aber nicht ausschließlich, folgende Bedingungen enthält: (1) ausschließliche Generierung und Speicherung von Schlüsselsätzen für Adobe-Signaturzertifikate auf einem Gerät mit dem Sicherheitsstandard FIPS 140-2 Level 2 und (2) nach Registrierung eines neuen Kontos oder immer dann, wenn ein neues AATL-Zertifikat für einen Abonnenten registriert wird, die Angabe wahrer und richtiger Informationen gegenüber DigiCert, wobei folgende Maßnahmen gefordert sind: (A) ein Kontoadministrator muss eine solide Identitätsprüfung durch persönlichen Kontakt mit DigiCert oder mittels eines gleichwertigen Sicherheitsverfahrens (z. B. über eine sichere Kommunikation per Video) durchführen, (B) ein Kontoadministrator muss eine solide Identitätsprüfung durch persönlichen Kontakt mit seinen Abonnenten (d. h. Endbenutzer) durchführen und die Aufzeichnung lokal zwecks Überprüfung speichern, bis DigiCert ein Online-System für Administratoren bereitstellt, mit dem Bestätigungen und Aufzeichnungen hochgeladen werden können, und (C) der Prozess zur Identitätsprüfung muss, unabhängig von der Eigenschaft als Administrator oder Abonnent, die Aufzeichnung des Abonnenten enthalten, die ihn selbst sowie einen gültigen, amtlichen Lichtbildausweis (z. B. Führerschein, Reisepass, Personalausweis usw.), der ein zum Abgleich geeignetes Foto des Abonnenten trägt, zeigt; sowie
- b. den Konditionen der entsprechenden CPS.

**28. Zusätzliche Einschränkungen für Code signing-Zertifikate.** Der Kunde ist in folgenden Fällen nicht berechtigt, ein Code signing-Zertifikat zu nutzen: (i) für oder im Auftrag eines Unternehmens, bei der es sich nicht um das Unternehmen des Kunden handelt; (ii) um Verfahren mit Private oder Public Keys in Verbindung einem Domain- und/oder eines Unternehmen-Namens durchzuführen, bei dem es sich nicht um den auf dem Zertifikatsantrag angegebenen Namen handelt; (iii) um verdächtigen Code zu verbreiten; oder (iv) in einer Weise, wodurch die Kontrolle über den oder der Zugang zu dem Private Key, der dem Public Key des Zertifikats entspricht, an Personen übertragen wird, bei denen es sich nicht um vom Kunden autorisierte Mitarbeiter handelt (eine solche Übertragung muss auf eine sichere Art und Weise durchgeführt werden, um den Private Key zu schützen).

**29. Zusätzliche Einschränkungen für nicht öffentliche TLS-/SSL-Zertifikate.** TLS-/SSL-Zertifikate, die mit einem privaten Root Certificate verkettet sind, dürfen nur mit Intranet-Domains verwendet werden und dürfen nicht Geräten zugeordnet werden, die über das Internet öffentlich zugänglich sind. QuoVadis behält sich das Recht vor, öffentlich zugängliche Internet-Server und/oder Geräte zu überwachen, um sicherzustellen, dass private TLS-/SSL-Zertifikate dieser Klausel entsprechen. Wenn QuoVadis die Nutzung privater TLS-/SSL-Zertifikate aufdeckt, die dieser Klausel nicht entsprechen, benachrichtigt QuoVadis den Kunden unverzüglich über diese Nichteinhaltung. Der Kunde muss das private TLS-/SSL-Zertifikat innerhalb von vierundzwanzig (24) Stunden (i) entweder auf eine Intranet-Domain verschieben; oder (ii) von den Kundenservern entfernen und revozieren. Wenn der Kunde die nicht konformen Zertifikate nicht revoziert oder entfernt, kann QuoVadis das Zertifikat revozieren.