

## 1. Vertragsgegenstand

- (1) Gegenstand dieses Vertrages ist die Auditierung des Informationssicherheits-Managementsystems (ISMS) des Kunden durch die Zertifizierungsstelle (OCG) und im Falle der Erfüllung der Bedingungen die Erreichung und Aufrechterhaltung einer Zertifizierung auf der Basis der Norm/des Regelwerkes

### ISO/IEC 27001 in der Fassung 2013

und die damit verbundene Überwachung des ISMS zur Aufrechterhaltung der Gültigkeit des Zertifikates sowie das Nutzungsrecht des OCG Zertifizierungszeichens für die Organisation

**>>antragstellende Organisation<<**

Zu zertifizierende(r) Standort(e)	Geltungsbereich (Prozesse/Services)

(Alle Standorte, für die die Zertifizierung gelten soll, müssen explizit hier angegeben werden und jeweils auch die zu zertifizierenden Bereiche.)

## 2. Grundlagen des Vertrags

- (1) Neben den Bestimmungen dieses Zertifizierungsvertrages gelten auch die als Anlagen zum Zertifizierungsvertrag angeführten „Richtlinien zur Benutzung der Kennzeichen“ (gemeinsam im folgenden "Vertrag" genannt).
- (2) Die OCG schuldet als Zertifizierungsstelle ausschließlich die vertraglich genau festgelegten Leistungen, die unter Beachtung der allgemein anerkannten Regeln (Stand der Technik) erbracht werden. Die OCG übernimmt keine Haftung für die Richtigkeit der den Aufträgen zugrundeliegenden Gesetze, Richtlinien und Normen.
- (3) Auf Antrag des Kunden um Zertifizierung eines ISMS nach ISO/IEC 27001 hat eine Prüfung der Voraussetzungen durch autorisierte Auditoren der OCG stattzufinden. Bei dieser Prüfung wird die Konformität mit den gültigen Bestimmungen der Norm festgestellt.
- (4) Diese Prüfung und die angegebenen Daten im Antragsformular bilden die Grundlage für diesen Vertrag. Der Kunde verpflichtet sich daher, alle Änderungen in Bezug auf diese Angaben der OCG umgehend bekannt zu geben.
- (5) Basierend auf den Angaben im Antragsformular und eventuell vorliegender zusätzlicher Informationen, die z.B. aus Telefonaten, E-Mails oder persönlichen Kundenkontakten stammen können, erstellt die OCG dem Kunden ein Angebot. Angebote der OCG sind, soweit nicht schriftlich etwas Anderes vereinbart wird, freibleibend und nicht

bindend. Ein beidseits verbindlicher Vertrag kommt erst mit dem Zugang der schriftlichen Auftragsbestätigung (beidseits unterzeichneter Vertrag) der OCG beim Kunden zustande.

### 3. Dauer des Vertragsverhältnisses

#### **Beginn**

- (1) Das Vertragsverhältnis beginnt mit dem Datum der Vertragsunterzeichnung zwischen Kunde und der OCG und endet mit dem Ende der Gültigkeitsdauer des Zertifikates. Nach Ablauf der Gültigkeit des Zertifikates verlängert sich das Vertragsverhältnis jedoch automatisch zu gleichen sonstigen Bedingungen um jeweils weitere drei Jahre, wenn zum jeweiligen Zeitpunkt der Verlängerung Einigkeit über die jeweils weiteren Entgelte zwischen Kunde und der OCG über die jeweils nächsten drei Jahre besteht.

#### **Ende**

- (2) Das Vertragsverhältnis endet durch Ablauf der Zeit, ohne dass es einer Kündigung bedarf. Vor Ablauf der 3-Jahresfrist wird dem Kunden auf Wunsch ein neues Angebot für die Aufrechterhaltung der Zertifizierung für die nächste dreijährige Periode erstellt.

#### **Vorzeitige Kündigung**

- (3) Das Vertragsverhältnis kann trotz Befristung und auch ohne Angabe von Gründen unter Einhaltung einer einmonatigen Kündigungsfrist jeweils zum Monatsletzten schriftlich vom Kunden gekündigt werden. Der Kunde hat dadurch jedoch keinerlei Anspruch auf teilweise oder vollständige Rückerstattung des vereinbarten Entgelts.

#### **Kündigung aus wichtigem Grund**

- (4) Das Vertragsverhältnis kann von beiden Vertragspartnern aus wichtigem Grund jederzeit und fristlos schriftlich gekündigt werden.

Ein wichtiger Grund für die Zertifizierungsstelle liegt insbesondere dann vor, wenn

- a) der Kunde wesentliche vertragliche Verpflichtungen verletzt,
- b) die Entgelte nicht innerhalb der von der Zertifizierungsstelle festgesetzten Frist trotz wiederholter schriftlichen Mahnung und Setzung einer Nachfrist entrichtet werden.

Ein wichtiger Grund für den Kunden liegt insbesondere dann vor, wenn

- c) die Zertifizierungsstelle die ihr zugänglich gemachten Informationen über die Organisation des Kunden missbräuchlich verwendet oder
- d) die Zertifizierungsstelle wesentliche vertragliche Verpflichtungen verletzt.

### 4. Fristen und Termine/Verzug

- (1) Die vertraglich vereinbarten Fristen und Termine beruhen auf Schätzungen des Arbeitsumfanges aufgrund der Angaben des Kunden. Diese Zeitangaben erlangen nur dann Verbindlichkeit, wenn sie von der OCG schriftlich ausdrücklich als „verbindlich“ festgelegt worden sind. Verzögerungen berechtigen den Kunden nicht zur Geltendmachung von Ansprüchen, egal aus welchem Rechtstitel.

- (2) Verbindlich festgelegte Fristen beginnen mit der vollständigen Übereinstimmung in allen Vertragsteilen und über sämtliche Bedingungen der Leistung und enden mit der Bereitstellung der Leistung durch die OCG. Sie verlieren ihre Verbindlichkeit, wenn sich der Auftraggeber mit seinen Verpflichtungen in diesem Vertrag. – aus welchen Gründen immer – in Verzug befindet.
- (3) Wird die Auftragserfüllung durch Umstände verzögert, die die OCG nicht zu vertreten hat (z.B. Betriebsstörungen, Streik, höhere Gewalt, Transporthindernisse etc.), ist die OCG unter Ausschluss von Gewährleistungen, Irrtumsanfechtungen und/oder Schadenersatzansprüche berechtigt, entweder vom Vertrag zurückzutreten oder die Frist angemessen zu verlängern. Dies gilt auch dann, wenn die Ereignisse zu einem Zeitpunkt eintreten, in dem sich die OCG bereits in Verzug befindet. Die OCG wird dies dem Kunden rechtzeitig mitteilen. Die OCG ist im Rücktrittsfall berechtigt, bis dahin erbrachte Teilleistungen gegenüber dem Kunden zu den dafür vereinbarten Preisen abzurechnen.
- (4) Werden durch Verschulden des Kunden Termine nicht eingehalten, so ist der Kunde verpflichtet, etwaige Kosten zu ersetzen, die der OCG dadurch entstehen.
- (5) Die Geschäftszeiten der OCG sind ausgenommen der gesetzlichen Feiertage und eventueller Betriebsferien Mo.-Do. 9:00-16:00 und Fr. 9:00-14:00.

## 5. Entgelte

...

## 6. Zahlungsbedingungen

...

## 7. Ablauf des Zertifizierungsverfahrens

- (1) Die OCG als Zertifizierungsstelle führt die Tätigkeiten des Zertifizierungsverfahrens entsprechend der Vorgaben der normativen Regelwerke (unter anderem der ISO/IEC 17021:2015) durch und stellt bei positivem Ergebnis ein Zertifikat aus.
- (2) Der Ablauf der Zertifizierung gliedert sich zeitlich wie folgt:
  - a. Stage1-Audit: Dokumentenaudit (entfällt bei Rezertifizierungen)
  - b. Stage2-Audit: Umsetzungsaudit (max. 6 Monate nach Stage 1 bzw. vor dem Ablauf der bestehenden Zertifizierung) um den Zustand des ISMS beim Kunden zu beurteilen)
  - c. Im Anschluss daran die Zertifizierungsentscheidung der OCG
  - d. In den 2 darauffolgenden Jahren mindestens 1 Überwachungsaudit jährlich mit anschließenden Entscheidungen über die Aufrechterhaltung der Zertifizierung.
- (3) Falls beim Audit Abweichungen von der Norm ISO/IEC 27001 gefunden werden, kann ein Nachaudit notwendig werden.
- (4) Die Beurteilung, ob ein positives Audit- und/oder ein positives Zertifizierungsergebnis vorliegt und/oder ob ein Nachaudit erforderlich ist, obliegt ausschließlich der OCG (Beschwerden und Einsprüche dagegen: siehe Punkt 11.).

- (5) Bei negativem Auditergebnis wird dem Kunden eine Nachfrist zur Mängelbehebung und allenfalls erneuten Auditierung eingeräumt. Der Kunde ist verpflichtet, die Ursachen von erkannten Nichtkonformitäten zu analysieren und geeignete Korrekturmaßnahmen zu planen und durchzuführen. Über die Angemessenheit der nötigen Maßnahmen zur Mängelbehebung und die Dauer der gewährten Frist entscheidet die Zertifizierungsstelle (üblicherweise 8 Wochen, bei Gefahr im Verzug ist aber auch eine kürzere Frist möglich). Der Kunde ist verpflichtet die Mängelbehebung spätestens bis zum Ablauf der gewährten Fristen der OCG zu melden und gegebenenfalls entsprechende Nachweise der OCG zur Verfügung zu stellen. Falls die Nachfrist durch den Kunde nicht genutzt wird oder die aufgezeigten Mängel nicht behebbar sind, gilt die Auditierung als negativ und die Zertifizierung somit als nicht erteilt bzw. zurückgezogen.
- (6) Im Falle einer positiven Zertifizierungsentscheidung aufgrund eines positiven Audits wird dem Kunden von der OCG ein Zertifikat übermittelt.
- (7) Die OCG führt in der Folge jährliche Überwachungsaudits durch, welche zur Aufrechterhaltung des Zertifikates erforderlich sind.
- (8) In besonderen, begründeten Ausnahmefällen – insbesondere im Falle gewichtiger und plausibler Beschwerden Dritter über die zertifizierte Organisation – kann auch kurzfristig ein (zusätzliches) Audit aus besonderem Anlass erforderlich werden (siehe auch Pkt. 5/(6) in diesem Vertrag). Die Feststellung der Erforderlichkeit liegt dabei im sachlich auszuübenden Ermessen der OCG.
- (9) Die OCG ist nicht verpflichtet, die Richtigkeit der ihr zur Verfügung gestellten Prüfgrundlagen oder von mündlichen Auskünften des Auftraggebers oder seiner Mitarbeiter zu überprüfen, sodass sie von der Richtigkeit solcher Angaben ausgehen darf.
- (10) Die OCG ist berechtigt, die Methode und die Art der Untersuchung nach sachgemäßem Ermessen selbst zu bestimmen.
- (11) Die OCG erbringt Prüfleistungen, soweit im Einzelfall nichts anderes vereinbart wird, mit einem Prüfer pro Fachgebiet. Für die Prüfung erforderliche oder nützliche Hilfsleistungen sind vom Kunden oder in dessen Namen von einem Dritten der OCG unentgeltlich zur Verfügung zu stellen. Der Kunde hat alle zumutbaren Anstrengungen zu unternehmen, die erforderlichen oder nützlichen Hilfeleistungen zur Verfügung zu stellen. Bei der Erbringung von solchen Hilfsleistungen hat der Kunde die Einhaltung der geltenden gesetzlichen oder behördlichen Vorschriften, insbesondere im Bereich des Arbeitnehmerschutzes sicherzustellen.

## **8. Gültigkeit des Zertifikates**

- (1) Die Gültigkeit des Zertifikates beträgt drei Jahre ab Ausstellungsdatum aufgrund positiver Zertifizierungsentscheidung, sofern sämtliche Bedingungen zur Aufrechterhaltung der Gültigkeit vom Kunden erfüllt werden.
- (2) Zwingende Voraussetzung zur Aufrechterhaltung der Gültigkeit des Zertifikates und der damit verbundenen Berechtigung zur Führung des Zertifikates und zur Nutzung des Zertifizierungslogos sind insbesondere die Durchführung eines jährlichen Überwachungsaudits mit positiver Überwachungsentscheidung sowie ein aufrechtes Vertragsverhältnis.

## 9. Obliegenheiten der OCG

- (1) Die OCG behandelt alle ihr zugänglich gemachten Informationen über die Organisation des Kunden streng vertraulich, wertet diese nur zu Zwecken des Vertragsgegenstandes aus und gibt diese nicht an Dritte weiter. Soweit die OCG durch Gesetz, Verordnung, Bescheid oder Anweisung einer Behörde verpflichtet ist, vertrauliche Informationen des Kunden gegenüber Dritten offen zu legen, wird der Kunde (sofern gesetzlich nicht anders geregelt) von der OCG im Voraus über diese Offenlegung informiert, es sei denn, dies ist vom Gesetz her geregelt. Wenn vertrauliche Informationen anderen Stellen zur Verfügung gestellt werden müssen (z.B. der Akkreditierungsstelle), dann wird der Kunde von dieser Maßnahme durch die OCG informiert.
- (2) Der Kunde kann die OCG von diesen Verpflichtungen der Vertraulichkeit schriftlich entbinden. Im Antragsformular sind die Informationen, die von der OCG veröffentlicht werden, sichtbar gekennzeichnet. Von der Norm ISO/IEC 17021 wird gefordert, dass die OCG folgende Informationen öffentlich zur Verfügung stellt: Name des Kunden, einschlägige normative Dokumente, den Zertifizierungsbereich und den geografischen Standort (z.B. Stadt und Land) oder den geografischen Ort des Hauptsitzes und jeden für den Kunden verfügbaren Standort innerhalb des Anwendungsbereiches einer Mehrfach-Standort-Zertifizierung. Die Zertifizierungsstelle muss im Fall von substantziellen Beschwerden zusammen mit dem Kunden und dem Beschwerdeführer ermitteln, ob, und falls, bis zu welchem Grad, der Gegenstand der Beschwerde sowie dessen Lösung öffentlich zugänglich gemacht werden muss.
- (3) Informationen, die aus anderer Quelle als vom Kunden stammen (Beschwerdeführer, Behörden), werden von der OCG vertraulich behandelt.
- (4) Die von der OCG benannten fachkompetenten Vertreter (Auditoren und/oder Experten bzw. falls notwendig Übersetzer und Dolmetscher) im Rahmen des Zertifizierungsprozesses unterliegen ebenfalls obig beschriebenen Grundsätzen der Vertraulichkeit, zu deren Einhaltung sie sich schriftlich verpflichtet haben.
- (5) Die OCG benennt fachkompetente Vertreter (Auditoren und/oder Experten) für die Durchführung jedes Audits. Die OCG informiert den Kunden über weitere Beschäftigungen dieser fachkompetenten Vertreter der OCG (zusätzlich zur Audittätigkeit) unter Angabe relevanter Informationen (z.B. Dienstgeber, Organisation/Unternehmen, Art der Beschäftigung etc.).
- (6) Sollte der Kunde mit der Wahl der Vertreter der OCG nicht einverstanden sein, so hat er die Möglichkeit, dies der OCG bis 7 Tage vor dem Audit, spätestens jedoch binnen 14 Tagen ab Kenntnis, schriftlich unter Angabe von Gründen mitzuteilen. Die OCG entscheidet im Anschluss neuerlich unter besonderer Würdigung der Interessen des Kunden über die Benennung fachkompetenter Vertreter.
- (7) Die OCG nimmt die notwendigen Prüfungen möglichst ökonomisch vor Ort während der regulären Betriebszeiten vor und verpflichtet sich, die dabei entstehenden Störungen des Betriebs des Auftraggebers möglichst gering zu halten.
- (8) Die OCG als Zertifizierungsstelle trifft unabhängig und weisungsfrei die Entscheidungen in Bezug auf die Zertifizierung, einschließlich der Erteilung, Aufrechterhaltung, Erneuerung, Erweiterung, Einschränkung, Aussetzung und Zurückziehung der Zertifizierung. Der Kunde erkennt dieses Recht der OCG ausdrücklich an.

- (9) Die OCG stellt nach dem Vorliegen aller notwendigen Erfordernisse das Zertifikat aus. Es entsteht kein Rechtsanspruch auf die Erteilung der Zertifizierung, diese darf jedoch nur aus sachlich gerechtfertigten Gründen verweigert werden.
- (10) Die OCG nimmt die zertifizierte Organisation nach positiver Zertifizierungsentscheidung und bis zum Zeitpunkt des Ablaufs der Gültigkeit der Zertifizierung bzw. Beendigung des Vertrages unter Angabe von Name, Firmensitz, Zertifizierungsgrundlage und Geltungsbereich in ihr veröffentlichtes Verzeichnis auf.
- (11) Die OCG unterrichtet nach Ausstellung des Zertifikates den Kunden über relevante Änderungen im Zertifizierungsverfahren, welche unmittelbare Auswirkungen auf den Kunden haben.
- (12) Die OCG gibt den Status der Zertifizierung des ISMS des Kunden auf Anfrage von Dritten wahrheitsgetreu als aufrecht, ausgesetzt, eingeschränkt, entzogen, zurückgezogen oder abgelaufen bekannt.

## 10. Obliegenheiten des Kunden

- (1) Der Kunde gewährt der OCG auf Wunsch kostenlos Zugang zu allen erforderlichen Materialien, Unterlagen und Informationen zur Einsichtnahme vor Ort und/oder teilweise bzw. teilweise auch Remote über entsprechend gesicherte elektronische Verbindungen, welche zur Erfüllung der sich aus dem Vertragsverhältnis ergebenden Verpflichtungen notwendig sind, insbesondere alle sich auf das ISMS beziehenden Unterlagen (Handbuch, Verfahrensanweisungen etc.). Der Kunde hat dazu der OCG bereits bei Auftragserteilung Zugang zu sämtliche erforderlichen Unterlagen wie Zeichnungen, Pläne, Berechnungen und Bescheinigungen zu gewähren, für sämtliche erforderliche Genehmigungen und Freigaben zu sorgen, jederzeit auftragsbezogene Auskünfte zu erteilen und vor Beginn der Prüfungen die hierzu notwendigen Vorbereitungen zu treffen, insbesondere das Prüfobjekt und die Dokumentationen dazu zugänglich zu machen. Der Kunde ist dazu verpflichtet, alle zumutbaren Anstrengungen zu unternehmen, die erforderlichen Unterlagen oder Genehmigungen rechtzeitig bereitzustellen. Kommt der Kunde diesen Pflichten trotz Setzung einer angemessenen Nachfrist durch die OCG nicht nach, so ist der Vertrag mit Ablauf dieser Frist aufgehoben. Die OCG ist in diesem Fall berechtigt, Schadenersatz wegen Nichterfüllung geltend zu machen.
- (2) Der Kunde verpflichtet sich, sämtliche als intern oder vertraulich gekennzeichnete Unterlagen und Informationen, die ihm im Zusammenhang mit diesem Vertrag zugänglich werden, geheim zu halten. Nach Vertragsbeendigung wird der Kunde sämtliche Unterlagen und Informationen, die er von der OCG erhalten hat, an diese zurückgeben und selbst keine Kopien davon behalten.
- (3) Der Kunde benennt einen Managementbeauftragten, welcher den Vertretern der OCG (Auditoren und/oder Experten) unentgeltlich zur Seite steht und bei deren Tätigkeiten in der Organisation des Kunden begleitet.
- (4) Der Kunde verpflichtet sich, dass seine Mitarbeiter den Auditoren der OCG wahrheitsgemäße Auskünfte über alle für die Beurteilung des zu zertifizierenden ISMS notwendigen Angaben im gewünschten Ausmaß erteilen werden.
- (5) Der Kunde gewährt den Vertretern der OCG (Auditoren und/oder Experten) und/oder Vertretern der Akkreditierungsstelle Zugang zu den betroffenen Organisationseinheiten

(Bereiche, Prozesse, Personal etc.) und Einsicht in die geforderten Aufzeichnungen (Geschäftsfälle, Firmenaufzeichnungen etc.).

- (6) Der Kunde ist verpflichtet, die Ursachen von erkannten Nichtkonformitäten zu analysieren und geeignete Korrekturmaßnahmen zu planen und durchzuführen sowie die OCG über den Status der Korrekturmaßnahmen zu informieren.
- (7) Der Kunde informiert die OCG umgehend über alle Veränderungen in der Organisation (z.B. Schließung von Standorten, Merger, Veränderung des Tätigkeitsbereiches oder des ISMS, Geltungsbereich etc.). Unterlassungen in der Informationsübermittlung werden bei Vorsatz und entsprechend großen Abweichungen vor allem vom ursprünglichen Geltungsbereich als missbräuchliche Verwendung des Zertifikats und der Zertifizierungszeichen gewertet und haben den Entzug des Zertifikats zur Folge. Bei Veränderungen, die nicht vorsätzlich der OCG nicht bekannt gegeben wurden, wird die OCG eine angemessene Nachfrist zur Anpassung (Änderung/Erweiterung/Einschränkung) der Zertifizierung setzen. Falls der Kunde diese Nachfrist nicht entsprechend nutzt, ist die OCG zu einem Aussetzen und in letzter Konsequenz auch zu einem Entzug des Zertifikats berechtigt.
- (8) Der Kunde gestattet der OCG Informationen über den Kunden – insbesondere den Zertifizierungsakt – auch Dritten (z.B. der Akkreditierungsstelle, internen Auditoren der OCG, dem Zertifizierungskomitee, dem Unabhängigkeitskomitee etc.) zur Verfügung zu stellen, soweit dies zur Aufrechterhaltung der Zertifizierungsbefugnis der OCG oder zur Behandlung von Einsprüchen und Beschwerden nötig ist.
- (9) Der Kunde verpflichtet sich, alles zu unterlassen, was die Unabhängigkeit des von der OCG eingesetzten Personals (insbesondere der Auditoren) gefährden könnte. Dies bezieht sich vor allem auf Angebote auf Anstellung, Beratertätigkeiten oder andere Aufträge an die Person direkt oder an Firmen, an denen die jeweilige Person direkt oder indirekt beteiligt ist.
- (10) Falls dem Kunden ein Interessenskonflikt hinsichtlich der Auditoren oder der Zertifizierung bekannt ist oder wird, so hat er die Verpflichtung, dies unverzüglich der OCG bekannt zu geben.
- (11) Ferner gestattet der Kunde der OCG Informationen über den Kunden, insbesondere den Zertifizierungsakt und Teile davon, ausschließlich im Rahmen der Leistungserbringung auch per E-Mail in geeignet geschützter Form an Mitarbeiter, Auditoren und Funktionäre der OCG zu versenden.
- (12) Der Kunde verpflichtet sich, alle Beanstandungen betreffend sein ISMS und deren Behebung aufzuzeichnen, zu archivieren und den Vertretern der OCG (Auditoren und/oder Experten) während des Audits aufzuzeigen.
- (13) Der Kunde verpflichtet sich, alle zur Aufrechterhaltung der Zertifizierung notwendigen Maßnahmen durchzuführen und das ISMS durch systematische Maßnahmen laufend zu verbessern und weiterzuentwickeln.
- (14) Der Kunde verpflichtet sich zur Einhaltung der im Anhang dargestellten „Richtlinien zur Benutzung der Kennzeichen im Rahmen der Zertifizierung von ISMS nach ISO/IEC 27001“.

## 11. Beschwerden und Einsprüche

- (1) Der Kunde hat die Möglichkeit, gegen Zertifizierungsentscheidungen oder gegen Handlungen oder Unterlassungen der OCG schriftlich Einspruch bei der OCG einzulegen. Neben einer negativen (Re-)Zertifizierungsentscheidung kann auch gegen eine allfällige Einschränkung, Erweiterung, Aussetzung oder Entzug einer aufrechten Zertifizierung, sowie gegen Auditberichte, Fristen oder Auflagen Einspruch eingelegt werden. Beschwerden könne wegen sonstiger Umstände wie z.B. Vorfälle bei Audits erhoben werden.
- (2) Die OCG gibt dem Kunden in diesem Fall eine aussagekräftige Begründung für ihre Zertifizierungsentscheidung, Handlung oder Unterlassung.

Kann keine zufriedenstellende Lösung gefunden werden oder ist das Entscheidungsgremium der OCG vom Einspruch oder der Beschwerde selbst direkt betroffen (Interessenskonflikt), wird der Einspruch oder die Beschwerde an das Unabhängigkeitskomitee bzw. unabhängige Experten – unter Beachtung der Regeln bezüglich der Vertraulichkeit – zur Entscheidungsfindung weitergeleitet. Wenn der Einspruch nach Beurteilung des Unabhängigkeitskomitees bzw. des unabhängigen Experten berechtigt ist, wird die Sache zur erneuten Behandlung an das Zertifizierungskomitee zurückverwiesen. Die Entscheidung dieser Neubehandlung ist innerhalb der Zertifizierungsstelle endgültig.

## 12. Einschränkung, Aussetzung und Entzug

- (1) Wenn die Zertifizierungsstelle zur Ansicht gelangt, dass das ISMS des Kunden den im Zertifikat beschriebenen Umfang nicht mehr erfüllt, kann die Zertifizierungsstelle das Zertifikat einschränken, aussetzen oder entziehen.
- (2) Weitere Gründe für den Entzug des Zertifikats sind Zahlungsrückstand des Kunden trotz wiederholter schriftlicher Mahnung unter Androhung des Zertifikatsentzugs und Setzung einer Nachfrist sowie schwere wiederholte missbräuchliche Verwendung des Zertifikates bzw. des Zertifizierungskennzeichens trotz Aufforderung der OCG zur Unterlassung durch den Kunden.
- (3) Dem Kunden wird dies unverzüglich schriftlich mitgeteilt und der Status des Zertifikates wird von der OCG unverzüglich veröffentlicht (z.B. auf [www.ocqcert.com](http://www.ocqcert.com)). Gegen Beschlüsse der Zertifizierungsstelle kann der Kunde Beschwerde führen (siehe Pkt. 11.).
- (4) Sobald der Kunde schriftlich davon informiert wurde, dass das Zertifikat eingeschränkt, ausgesetzt oder widerrufen wurde, ist es ihm unverzüglich untersagt, weiter mit dem ursprünglichen Zertifikat zu werben oder darauf im Geschäftsverkehr zu verweisen. Der Kunde verpflichtet sich, bei Entzug keine Unterlagen mehr weiterzugeben, die auf das Zertifikat verweisen. Der Kunde verpflichtet sich weiters, binnen 6 Monaten nach Entzug alle auf die Zertifizierung verweisenden Unterlagen aus dem Verkehr zu bringen, soweit sich diese noch im Einflussbereich des Kunden befinden bzw. insoweit dies keinen unverhältnismäßig hohen Aufwand (mehr als 5.000,- EUR) verursachen würde. Bei Überschreitung dieser Frist oder nachweislicher wiederholter missbräuchlicher Verwendung des Zertifikates oder des Zertifizierungskennzeichens trotz Aufforderung zur Unterlassung durch die OCG, ist die OCG berechtigt, eine Konventionalstrafe in der Höhe der oben angeführten Kosten des (Re-) Zertifizierungsaudits max. jedoch 10.000,- EUR dem Kunden in Rechnung zu stellen.



**13. Gewährleistung**

...

**14. Haftung**

...

**15. Räumliche Geltung und Vertragsänderungen**

...

**16. Urheberrechte, Geheimhaltung, Vertraulichkeit und  
Datenschutz**

...

**17. Salvatorische Klausel**

...

**18. Rechtswahl, Gerichtsstand**

...

**19. Unterschriften der Vertragsparteien**

Auszug Zertifizierungsvertrag

**Anhang:**

---

# Richtlinien zur Benutzung der Kennzeichen

---

im Rahmen der Zertifizierung von ISMS  
nach ISO/IEC 27001:2013

**Österreichische Computer Gesellschaft (OCG)**

Wollzeile 1, 1010 Wien

[www.ocg.at](http://www.ocg.at)

# Inhalt

1. Eigentümer der Kennzeichen (Lizenzgeber, Zertifizierungsstelle).....	2
2. Benutzer der Kennzeichen (Lizenznehmer, Auftraggeber) .....	2
3. Gegenstand .....	2
4. Grundlage.....	3
5. Rechte und Pflichten .....	3
6. Aussetzung/Beendigung der Zertifizierung, Reduzierung des Geltungsbereiches .	4
7. Änderungen .....	5
8. Zuwiderhandlung .....	5

## 1. Eigentümer der Kennzeichen (Lizenzgeber, Zertifizierungsstelle)

- (1) Eigentümer der Kennzeichen ist die:  
Österreichische Computer Gesellschaft (OCG) [ZVR-Zahl 125777049]  
A-1010 Wien, Wollzeile 1; Tel: 01/512 02 35, Fax: 01/512 02 35-59  
E-Mail: [ocg@ocg.at](mailto:ocg@ocg.at); Website: [www.ocg.at](http://www.ocg.at) bzw. [www.ocgcert.com](http://www.ocgcert.com)  
im Folgenden „OCG“ genannt

## 2. Benutzer der Kennzeichen (Lizenznehmer, Auftraggeber)

- (1) Lizenznehmer der Kennzeichen sind die Auftraggeber/Kunden der OCG Zertifizierungsstelle, denen die Benutzung der Kennzeichen vertraglich gestattet wurde.

## 3. Gegenstand

- (1) Gegenstand sind folgende geschützte Kennzeichen:
- a) die Zertifizierungsurkunde
  - b) das Logo der Zertifizierungsstelle wie hier abgebildet: („Zertifizierungslogo OCG-Certification“)



- (2) Ausdrücklich untersagt wird die Verwendung der Zeichen (Logos) von akkreditierten Zertifizierungsstellen durch den Lizenznehmer (Bundesadler inkl. A der „Akkreditierung Austria“ – siehe auch Akkreditierungszeichenverordnung, AkkZV 2013).

## 4. Grundlage

- (1) Voraussetzung für die Benutzung der Kennzeichen durch Organisationen ist ein gültiger Vertrag über die Zertifizierung, Überwachung oder Rezertifizierung der betreffenden Organisation und der aufrechte gültige Status des Zertifikats. Das Recht zur Nutzung der Kennzeichen endet spätestens mit dem Ende des Vertragsverhältnisses.

## 5. Rechte und Pflichten

- (1) Die OCG erteilt dem Lizenznehmer eine
- nicht ausschließliche,
  - nicht übertragbare,
  - zeitlich an die Gültigkeit des Zertifikats gebundene
- Lizenz zur Benutzung der geschützten Kennzeichen.
- (2) Der Lizenznehmer darf die Kennzeichen zu geschäftlichen Zwecken auf Unterlagen der geschäftlichen Korrespondenz (z.B. Briefpapier, Visitenkarten, E-Mail) und im Rahmen der Werbung (z.B. Firmenfahrzeuge, Webseite, Prospekte) und zur Vertrauensbildung in der Unternehmenskommunikation gegenüber Geschäftspartnern und der Öffentlichkeit in der festgelegten Form benutzen.
- (3) Die Lizenz zur Benutzung der Kennzeichen ist beschränkt auf den von der OCG festgelegten Geltungsbereich der Zertifizierung der Organisation. Die Nutzung der Kennzeichen für nicht zertifizierte Bereiche des Lizenznehmers ist nicht gestattet. Sollten nur einzelne Bereiche zertifiziert worden sein, darf das Zertifikat nur in unmittelbarer Verbindung mit dem zertifizierten Bereich der Organisation verwendet werden.
- (4) Der Lizenznehmer muss bei der Benutzung der Kennzeichen
- a. auf die OCG als Zertifizierungsstelle,
  - b. den Geltungsbereich der Zertifizierung und
  - c. die Zertifizierungs-/Registrierungsnummer des Zertifikats hinweisen.

- (5) Jede irreführende, missbräuchliche oder das Vertrauen in
  - a. die Zertifizierung,
  - b. die Zertifizierungsstelle oder
  - c. das Zertifizierungssystemschädigende Verwendung der Kennzeichen ist streng untersagt.
- (6) Der Lizenznehmer trägt die Verantwortung für die Einhaltung der gegenständlichen Richtlinie durch seine Mitarbeiter.
- (7) Die Kennzeichen dürfen ausschließlich in der unter Punkt 3 dargestellten und von der OCG zur Verfügung gestellten Form benutzt werden. Jede Veränderung der Kennzeichen ist untersagt, mit Ausnahme der Skalierung unter Wahrung der proportionalen Größenverhältnisse. Das Kennzeichen muss leicht lesbar und deutlich sichtbar sein.
- (8) Ausdrücklich untersagt ist die Verwendung der Kennzeichen auf Laborprüfberichten, Kalibrierscheinen oder Inspektionsberichten.
- (9) Die Kennzeichen dürfen nicht auf Produkten oder Produktverpackungen verwendet werden. Insbesondere untersagt ist die Verwendung im Zusammenhang mit Produkten, Prozessen oder Dienstleistungen, durch die der Eindruck entstehen könnte, dass die Produkte, Prozesse oder Dienstleistungen selbst zertifiziert seien. Vielmehr muss aus der Verwendung erkennbar sein, dass die Zertifizierung für eine Organisationseinheit gilt bzw. dass die Produkte oder Dienstleistungen aus dem im Zertifikat bezeichneten Bereich stammen.
- (10) Die OCG hat das Recht und die Pflicht, die Verwendung der Kennzeichen durch den Lizenznehmer zu kontrollieren. Bei irreführender Verwendung der Zertifizierungsdokumente und Kennzeichen, fehlerhaften Verweisen bezogen auf den Zertifizierungsstatus etc. wird die OCG Korrekturen bzw. Gegenmaßnahmen verlangen. Sollten diese Maßnahmen nicht im erforderlichen Ausmaß wirksam sein, kann das ein Grund für die Vertragskündigung durch die OCG nach Pkt. 3/(4) des Zertifizierungsvertrages sein und zur Verhängung einer Konventionalstrafe nach Pkt. 12/(4) des Zertifizierungsvertrages führen.

## **6. Aussetzung oder Beendigung der Zertifizierung, Reduzierung des Geltungsbereiches**

- (1) Wird die Zertifizierung entsprechend den Zertifizierungsregeln der OCG
  - a) ausgesetzt,
  - b) widerrufen oder
  - c) durch Ablauf der Gültigkeitsdauer ungültig,

so verliert der Lizenznehmer das Recht auf Benutzung der Kennzeichen.  
In diesem Fall darf der Lizenznehmer noch vorhandene Materialien und Medien noch höchstens sechs Monate nach Erlöschen der Gültigkeit des Zertifikats benutzen.

- (2) Wird das Vertragsverhältnis (aus welchen Gründen auch immer) beendet, so erlischt die Lizenz zur Nutzung der Kennzeichen mit sofortiger Wirkung.
- (3) Wird der Geltungsbereich des Zertifikats eingeschränkt, so hat der Lizenznehmer dies auf allen Unterlagen und Werbematerialien innerhalb von drei Monaten entsprechend richtigzustellen.

## **7. Änderungen**

- (1) Die OCG wird den Lizenznehmer über allfällige Änderungen dieser Richtlinie in Kenntnis setzen und der Lizenznehmer hat diese binnen einer angemessenen Frist, spätestens aber innerhalb von 12 Monaten einzuhalten und umzusetzen.

## **8. Zuwiderhandlung**

- (1) Bei missbräuchlicher Verwendung, insbesondere entgegen einer Bestimmung des Umfangs des Nutzungsrechtes durch den Lizenznehmer wird das Recht des Lizenznehmers, die Kennzeichen zu nutzen, mit sofortiger Wirkung ausgesetzt.
- (2) Jede von dieser Richtlinie abweichende Verwendung der Kennzeichen ist umgehend und auf Kosten des Lizenznehmers zu beseitigen.
- (3) Werden die Kennzeichen durch den Kunden missbräuchlich verwendet oder die Richtlinien nachweislich und trotz Aufforderung durch die OCG auf Unterlassung wiederholt missachtet, kann es zur Vertragsauflösung oder zur Verhängung einer im Zertifizierungsvertrag vereinbarten Konventionalstrafe kommen (siehe Zertifizierungsvertrag Pkt. 12/(4) bzw. Pkt. 5/(10) in diesen Richtlinien zur Benutzung der Kennzeichen).