German

Anforderungen an die Informationssicherheit für Anbieter

1. Einleitung

Die vorliegenden Bedingungen und Bestimmungen („**Informationssicherheitsanforderungen**“) stehen für die erforderlichen Informationssicherheitsmaßnahmen („**technische und organisatorische Sicherheitsmaßnahmen**“), welche für den Anbieter (wie nachstehend definiert), dessen Unterauftragnehmer sowie für sämtliche Zeitarbeitskräfte, Auftragnehmer oder zusätzliche Lieferanten des Anbieters und/oder im dessen Auftrag handelnde Vertreter (nachstehend zusammen als „**Dritte**“ bezeichnet) gelten, die im Auftrag von, für und/oder über den Anbieter Dienstleistungen erbringen bzw. Produkte liefern und/oder sonstigen Verpflichtungen nachkommen, wozu jede der nachstehenden zählt:

a. Die Erfassung, Speicherung, Handhabung oder Entsorgung von Ressourcen im Zusammenhang mit vertraulichen Informationen (wie nachstehend definiert) von CWT (wie nachstehend definiert);
b. Die Bereitstellung oder Unterstützung von CWT-markengeschützter Dienstleistungen und Produkte über nicht zu CWT gehörige Systeme oder andere Ressourcen;
c. Die Konnektivität zu CWTs vertraulichen Informationsressourcen;
d. Die beiläufige und/oder von CWT bezahlte Entwicklung von Software, soweit diese von bzw. im Auftrag des Anbieters produziert oder entwickelt wird oder einen Teil einer Software darstellt – gemäß dem Vertrag (wie nachstehend definiert), dem die vorliegenden technischen und organisatorischen Sicherheitsmaßnahmen beiliegen (einschließlich aller etwaigen Leistungsbeschreibungen, Anlagen, Bestellungen oder sonstigen Dokumente, die gemäß dem Vertrag gelten bzw. diesem unterstehen bzw. sich auf diesen beziehen) –, für deren Entwicklung von CWT Gelder verlangt worden sind; oder
e. das Hosting und die Entwicklung von Websites für CWT und/oder CWTs Kunden.

2. Definitionen

Sofern nicht anderweitig in diesem Dokument dargelegt oder ergänzt, haben die hier definierten Begriffe dieselbe Bedeutung wie im Hauptvertrag. Die nachstehenden definierten Begriffe gelten für die vorliegenden Informationssicherheitsanforderungen.

„**Verbundene Unternehmen**“ sind jene, mit Bezug auf eine Vertragspartei, auf eine Gesellschaft oder eine sonstige juristische Person, die: (i) entweder direkt oder indirekt eine Vertragspartei beherrscht; oder (ii) direkt oder indirekt von einer Vertragspartei beherrscht wird; oder (iii) direkt oder indirekt von einer Gesellschaft oder einer juristischen Person, die direkt oder indirekt eine Vertragspartei beherrscht, beherrscht wird. Zu diesem Zwecke steht „Beherrschung“ für das Recht, mehr als fünfzig Prozent (50 %) des Stimmrechts oder eines ähnlichen Besitzrechts auszuüben, jedoch nur solange, wie die genannte Beherrschung besteht.

„Vertrag“ steht für die Vereinbarung oder ein sonstiges Rechtsdokument, welche bzw. welches CWT und der Anbieter eingehen bzw. abschließen.

„Geschützte Unternehmensdaten“ beziehen sich auf jene Daten, die für (a) CWT und dessen verbundene Unternehmen, für (b) einen Kunden von CWT oder für (c) Mitarbeiter von CWT unter Umständen einen ernstzunehmenden Verlust oder eine Unterbrechung der Geschäftstätigkeit bedeuten oder die genannten Personengruppen unter Umständen in Verlegenheit bringen würden. Zu diesen Daten zählen Kunden- oder Lieferantenlisten; individuelle Informationen von Reisenden; Geschäftskontonummern von Unternehmen; Nummern von nicht auf Kreditkarten basierenden, markengeschützten Geschenkgutscheinen oder Geldkarten; Loyalitätsdaten von Kunden, die nicht zu personenbezogenen Daten (wie nachstehend definiert) gehören; Geschäftsgeheimnisse, Kundencodes; Leistungsbewertungen; Verträge, Ausschreibungen, Anfragen um Angebote oder Informationen; strategische Pläne, Marketingpläne, Fusionen, Übernahmen und Veräußerungen sowie Finanzaufstellungen.

„Vertrauliche Informationen“ beziehen sich auf jegliche geschäftlich sensiblen, geschützten oder anderweitig vertraulichen Informationen, die sich auf CWT, dessen verbundene Unternehmen oder auf den Inhalt und/oder den Zweck des Vertrags beziehen, welche auf mündlichem, schriftlichem oder sonstigem Wege direkt oder indirekt in den Besitz des Anbieters bzw. in den Besitz eines Mitarbeiters bzw. von Mitarbeitern, Vertretern, Auftragnehmern oder Unterauftragnehmern des Anbieters infolge bzw. im Zusammenhang mit dem Vertrag gelangen. Hinweis: Alle Arbeitsergebnisse gelten als vertrauliche Informationen.

„CWT“ bezieht sich auf das Unternehmen Carlson Wagonlit Travel, wie in dem Vertrag dargestellt, sowie auf dessen verbundene Unternehmen.

„**Demilitarisierte Zone**“ bzw. „**DMZ**“ steht für ein Netzwerk bzw. ein Subnetzwerk, das zwischen einem vertrauenswürdigen internen Netzwerk, wie einem privaten oder firmeninternen LAN (Local Area Network), und einem nicht vertrauenswürdigen Netzwerk, wie dem öffentlichen Internet, sitzt. Mit einer DMZ wird verhindert, dass externe Nutzer direkten Zugang auf interne Systeme oder sonstige Ressourcen erhalten.

„Prozess für das Störfallmanagement“ bezieht sich auf einen vom Anbieter entwickelten und dokumentierten Prozess und Ablauf, der im Falle eines Ereignisses im Sinne eines tatsächlichen oder vermuteten Angriffs, Eindringens, unbefugten Zugriffs, Verlustes oder eines sonstigen Verstoßes in Bezug auf die Vertraulichkeit, Verfügbarkeit oder Integrität der vertraulichen Informationen von CWT Anwendung findet.

„Maskierung“ beschreibt den Vorgang zur Verdeckung von auf einem Bildschirm angezeigten Informationen.

„Mobile und tragbare Geräte“ beziehen sich auf mobile und/oder tragbare Computer, Geräte, Datenträger und Systeme, die problemlos getragen, bewegt, transportiert oder befördert werden können und in Verbindung mit dem Vertrag genutzt werden. Zu diesen Geräten zählen beispielhaft Laptops, Tablets, USB-Festplatten, USB-Speichersticks, Personal Digital Assistants (PDAs), Mobil- bzw. Datentelefone und alle sonstigen drahtlosen Geräte bzw. Peripheriegeräte, auf denen vertrauliche Informationen gespeichert werden können.

„Personenbezogene Daten“, wie gemäß der EU-Richtlinie 94/46/EG sowie gemäß sonstigen weltweit anwendbaren Gesetzen zur Informationssicherheit, dem Datenschutz und dem Schutz der Privatsphäre definiert, sind Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Hierzu gehören insbesondere: vollständiger Name (einschließlich Prä- und Suffix), persönliche Identifikationsnummer (PIN) oder Passwort, Zahlungskarteninformationen oder damit verbundene Nummern (z. B. CVV-Code), Bankkontoinformationen, E-Mail-Adressen, Telefonnummer, Wohnanschrift, Informationen mit Aussagekraft über den Gesundheitsstatus (z. B. vorherige Behandlungen) oder über Gesundheitsanforderungen, Reisedokumente wie Führerscheinnummer, Personalausweisnummer, Reisepassnummer, Staatsangehörigkeit, Wohnsitz, Geburtsdatum, sexuelle Orientierung, Religion, Gewerkschaftsmitgliedschaft, Sozialversicherungsnummer oder Visumnummer, Vorstrafen, biometrische oder genetische Daten.

„Sicherheitsgateway“ bezieht ich auf eine Reihe von Kontrollmechanismen zwischen zwei oder mehr Netzwerken mit unterschiedlichen Vertrauensstufen, mithilfe derer Traffic, der zwischen den Netzwerken und den dazugehörigen administrativen Servern und Verwaltungsservern vorbeikommt oder versucht vorbeizukommen, gefiltert und protokolliert wird. Beispiele für Sicherheitsgateways sind Firewalls, Firewall-Verwaltungsserver, Hop Boxes, Session Border Controller, Proxyserver und Intrusion-Prevention-Systeme.

„Starke Authentifizierung“ steht für den Einsatz von Mechanismen und Methoden zur Authentifizierung, welche stärker als die dabei erforderlichen Passwörter sind. Beispielhaft wären in diesem Zusammenhang digitale Zertifikate, die Zwei-Faktor-Authentifizierung und Einmalpasswörter zu nennen.

„Starke Verschlüsselung“ steht für den Einsatz von Verschlüsselungstechniken mit einer Mindestschlüssellänge von 256 Bits für die symmetrische Verschlüsselung und 1024 Bits für die asymmetrische Verschlüsselung, deren Stärke in ausreichendem Maße dafür sorgt, dass verschlüsselte Informationen vor unbefugtem Zugriff geschützt sind, und deren Stärke zudem für den Schutz der Vertraulichkeit und Geheimhaltung der verschlüsselten Daten ausreichend ist; dies gilt einschließlich einer dokumentierten Richtlinie zur Verwaltung der Verschlüsselungsschlüssel und der damit verbundenen Prozesse, welche geeignet ist, die Vertraulichkeit und Geheimhaltung der Schlüssel und Passwörter, welche als Eingaben zum Verschlüsselungsalgorithmus verwendet werden, zu schützen. Zur starken Verschlüsselung zählen insbesondere: SSL ab Version 3.0/TLS ab Version 1.0, Point-to-Point Tunneling Protocol (PPTP), AES 256, FIPS 140-2 (nur für US-Regierung), RSA mit 1024-Bit-Schlüssel, SHA1/SHA2/SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric Version 4 oder WPA2.

„Technische und organisatorische Sicherheitsmaßnahmen“ beziehen sich auf alle im Rahmen der vorliegenden Informationssicherheitsanforderungen erforderlichen Aktivitäten , um auf Informationen oder Daten zuzugreifen, diese zu verwalten, zu übertragen, zu verarbeiten, zu speichern, aufzubewahren oder zu vernichten; um die gemäß dem Vertrag und gemäß den sonstigen anwendbaren Datenschutzgesetzen betroffenen Parteien offenzulegen und zu benachrichtigen; sowie um Informationen und Daten zu sichern, um deren Verfügbarkeit, Integrität, Vertraulichkeit und Geheimhaltung sicherzustellen bzw. um Personen über die Nichtsicherung dieser Daten und Informationen zu unterrichten. Zu den Maßnahmen zählen insbesondere jene, welche nach den EU-Richtlinien 94/46/EG und 2006/24/EG, wie in den Mitgliedsstaaten jeweils bekanntgegeben, dem United States Gramm-Leach Bliley Act (GLBA), dem United States Health Insurance Portability and Accountability Act (HIPAA), den Datenschutzanforderungen der EU/Schweiz und nach allen sonstigen internationalen und US-amerikanischen Gesetzen, nach offizieller Rechtsauslegung oder Leitsatzentscheidungen, welche sich auf Informationen oder Daten gemäß dem Vertrag beziehen, erforderlich sind bzw. der Auslegung nach erforderlich sind.

„**Dritter“** bezieht sich auf Unterauftragnehmer sowie auf Zeitarbeitskräfte, Auftragnehmer oder zusätzliche Lieferanten des Anbieters und/oder in dessen Auftrag handelnde Vertreter, einschließlich der Definition eines Dritten gemäß anwendbarem EU-, US- oder sonstigem internationalen Recht.

„**Anbieter**“ bezieht sich auf den im Vertrag genannten Auftraggeber zusammen mit dessen verbundenen Unternehmen.

Solange der Anbieter Zugriff auf CWTs vertrauliche Informationen hat, verpflichtet sich dieser zur Einführung vernünftiger und angemessener technischer und organisatorischer Sicherheitsmaßnahmen in Einklang mit den für die Informationssicherheit geltenden Best Practices, um die Integrität, Verfügbarkeit und Vertraulichkeit der Informationen zu schützen.

Der Anbieter sichert zu und gewährleistet, dass er sich an die nachstehenden technischen und organisatorischen Sicherheitsmaßnahmen halten wird, soweit diese auf die Bereitstellung der in dem vorliegenden Vertrag genannten Dienstleistungen anwendbar sind.

3. Organisation der Informationssicherheit

3.1 Der Anbieter verpflichtet sich, angemessene Richtlinien und ein Programm zu organisatorischen, operativen, administrativen, physischen sowie technischen und organisatorischen Sicherheitsmaßnahmen festzusetzen, umzusetzen und aufrechtzuerhalten, welche geeignet sind, um (1) den Zugriff auf die vertraulichen Informationen von CWT zu verhindern, welcher in einer Art und

Weise stattfindet, die gemäß dem Vertrag bzw. den vorliegenden Informationssicherheitsanforderungen nicht zulässig ist, und (2) alle anwendbaren Industriestandards einzuhalten. Des Weiteren hat der Anbieter sicherzustellen, dass alle seine mit der Sicherheit betrauten Mitarbeiter über die notwendige Erfahrung auf dem Gebiet der Informationssicherheit verfügen.

3.2 Der Anbieter verpflichtet sich, im Hinblick auf die technischen und organisatorischen Sicherheitsmaßnahmen gegenüber Dritten von ihm, die Zugang zu CWTs vertraulichen Informationen benötigen, für ein angemessenes Maß an Überwachung, Anleitung und Schulung zu sorgen. Der Anbieter verpflichtet sich, Schulungen in Bezug auf die technischen und organisatorischen Sicherheitsmaßnahmen bei Einstellung und vor Zugriff auf die vertraulichen Informationen von CWT durchzuführen. Schulungen zur Auffrischung sollten mindestens einmal jährlich stattfinden und so zeitnah wie möglich, nachdem es zu wesentlichen Änderungen hinsichtlich der technischen und organisatorischen Sicherheitsmaßnahmen des Anbieters gekommen ist.

3.3 Dritte des Anbieters mit wesentlichen sicherheitsrelevanten Aufgaben, darunter u. a. HR- und IT-Funktionen, sowie alle Technologie-Administratoren-Funktionen erhalten eine konkret auf ihre jeweilige Funktion zugeschnittene Sondereinweisung. Dazu gehören, wie auf die jeweilige Funktion anwendbar, Informationssicherheitsverfahren, akzeptable Verwendung von Informationssicherheitsressourcen, aktuelle Bedrohungen für Informationssysteme, Sicherheitsfunktionen bestimmter Systeme sowie sichere Zugriffsverfahren.

3.4 Der Anbieter verpflichtet sich, vernünftige Maßnahmen zu ergreifen, um den unbefugten Zugriff auf die vertraulichen Informationen von CWT bzw. den Verlust dieser sowie zu den Diensten, Systemen, Geräten oder Datenträgern, auf denen sich diese Informationen befinden, zu verhindern.

3.5 Der Anbieter verpflichtet sich, Prozesse und Verfahren zur Risikobewertung einzusetzen, um in regelmäßigen Abständen die Systeme, welche zur Bereitstellung von Dienstleistungen oder Produkten gegenüber CWT eingesetzt werden, zu bewerten. Der Anbieter wird etwaige Risiken so schnell wie vernünftigerweise möglich und entsprechend der Höhe des Risikos, welche für die vertraulichen Informationen angesichts der Bedrohungen, die zum Zeitpunkt der Entdeckung bekannt sind, gilt, beseitigen. Des Weiteren wird der Anbieter ein Verfahren betreiben, wonach es den Dritten des Anbieters möglich ist, Risiken bzw. vermutete Störfälle dem Sicherheitsteam des Anbieters zu melden.

3.6 Soweit die Dritten des Anbieters Dienstleistungen gemäß dem Vertrag in CWT-Einrichtungen erbringen oder Dienste, Systeme, Geräte oder Datenträger nutzen, von denen CWT der Eigentümer ist bzw. die von CWT betrieben oder verwaltet werden, verpflichtet sich der Anbieter zur Einhaltung sämtlicher Richtlinien von CWT, die diesem bereitgestellt werden und für den jeweiligen Zugang gelten. Der Anbieter verpflichtet sich, dafür Sorge zu tragen, dass Dritte von ihm, welche die Einrichtungen, Dienste, Systeme, Geräte oder Datenträger von CWT nutzen, um gemäß dem Vertrag Dienstleistungen zu erbringen, alle anwendbaren Richtlinien von CWT einhalten werden. Ferner verpflichtet sich der Anbieter, CWT umgehend schriftlich zu informieren, sollte ein Zugriff in der hier beschriebenen Art nicht länger notwendig sein, wenn beispielsweise ein Mitarbeiter, Auftragnehmer, Unterauftragnehmer oder ein Dritter des Anbieters im Rahmen des Vertrags nicht länger Dienstleistungen erbringt bzw. nicht mehr auf CWTs vertrauliche Informationen zugreift.

3.7 Der Anbieter verpflichtet sich, zu den zu ihm gehörigen Ressourcen, welche auf die vertraulichen Informationen von CWT zugreifen bzw. diese übertragen, verwalten, speichern oder verarbeiten, Aufzeichnungen zu führen.

3.8 Der Anbieter verpflichtet sich zur Einhaltung der Anforderungen von CWT zu Hintergrundprüfungen, soweit diese gesetzlich erforderlich und erlaubt sind, und so wie diese anderenfalls in einer entsprechenden Leistungsbeschreibung/Bestellung/einem entsprechenden Arbeitsauftrag beschrieben sind.

4. Physische Sicherheit und Umgebungssicherheit

4.1 Der Anbieter verpflichtet sich, dafür Sorge zu tragen, dass alle seine Systeme und sonstigen Ressourcen, welche für die Verwendung durch mehrere Nutzer vorgesehen sind, sich in sicheren physischen Einrichtungen befinden, zu denen ausschließlich befugte Personen Zugang haben.

4.2 Der Anbieter verpflichtet sich, zu Prüfungszwecken den Zugang zu den physischen Einrichtungen, in denen sich Systeme und sonstige Ressourcen befinden, welche für die Verwendung durch mehrere Nutzer vorgesehen sind und in Verbindung mit der Erbringung der Leistungen des Anbieters gemäß dem Vertrag genutzt werden, zu überwachen und aufzuzeichnen.

4.3 Der Anbieter verpflichtet sich, dafür zu sorgen, dass Dritte von ihm einen Geheimhaltungsvertrag bzw. eine Verschwiegenheitserklärung unterzeichnen, und zwar bevor es zum Zugriff auf die vertraulichen Informationen von CWT kommt.

4.4 Der Anbieter verpflichtet sich, dafür Sorge zu tragen, dass alle seine Mitarbeiter auf einen aufgeräumten Arbeitsplatz achten und vor Verlassen des Arbeitsbereiches ihre Bildschirme sperren.

4.5 Der Anbieter verpflichtet sich zur Erfassung sämtlicher Unternehmensvermögenswerte bei Beendigung des Beschäftigungsverhältnisses bzw. des Vertrags.

4.6 Der Anbieter verpflichtet sich, den physischen Zugang zu seinen Einrichtungen gemäß den nachstehenden Bedingungen zu beschränken und zu überwachen:

a. Der Zugang von Besuchern wird protokolliert, wobei das Protokoll einschließlich des Namens des Besuchers, des durch ihn vertretenen Unternehmens und des Namens des Mitarbeiters, der den physischen Zugang befugt hat, drei Monate lang aufzubewahren ist.
b. Der Zugang ist auf das entsprechende Personal beschränkt, beruhend auf den jeweiligen Arbeitsanforderungen.
c. Alle Mitarbeiter müssen ein vom Unternehmen bereitgestelltes Namensschild tragen.

d. Die Zugangsberechtigung wird bei Kündigung umgehend aufgehoben, wobei alle physischen Zugangsmechanismen wie Schlüssel, Zugangskarten usw. zurückzugeben bzw. zu deaktivieren sind.
e. Das Rechenzentrum bzw. der Computerraum ist verschlossen und der Zugang auf diejenigen Personen beschränkt, die Zugang benötigen.
f. Soweit gesetzlich zulässig mithilfe von Videokameras zur Überwachung der einzelnen physischen Zugänge zu sensiblen Bereichen sowie die regelmäßige Überprüfung dieser Daten. Das Videomaterial ist für einen Zeitraum von mindestens drei (3) Monaten aufzubewahren.
g. Geräte zur Speicherung, Verarbeitung oder Übertragung personenbezogener Daten müssen physisch abgesichert sein, darunter drahtlose Zugriffspunkte, Gateways, tragbare Geräte, Netzwerk-/Kommunikationshardware und Telekommunikationsleitungen.

4.7 Der Anbieter verpflichtet sich, Kontrollen einzuführen, um das Risiko physischer Bedrohungen zu minimieren und vor diesen zu schützen.

4.8 Der Anbieter verpflichtet sich, sämtliche Hardware-Assets zur Bearbeitung oder Verarbeitung vertraulicher Informationen von CWT in Übereinstimmung mit den empfohlenen Wartungsanforderungen des externen Service-Providers zu warten.

4.9 Der Anbieter verpflichtet sich, Konferenzraum- und sonstige öffentlich zugängliche Netzwerkdosen vom Netzwerk des Anbieters logisch zu begrenzen sowie lediglich auf authentifizierte Nutzer zu beschränken bzw. standardmäßig zu deaktivieren.

4.10 Der Anbieter verpflichtet sich, Geräte, mit denen per direkter physischer Interaktion Daten von Zahlungskarten erfasst werden, vor Manipulation und Austausch zu schützen, indem er in regelmäßigen Abständen die Geräteoberflächen auf Manipulations- und Austauschversuche prüft und seine Mitarbeiter hinsichtlich des Erkennens von Manipulations- oder Austauschversuchen schult.

4.11 Der Anbieter verpflichtet sich, Zugangspunkte wie Anliefer- und Ladezonen und sonstige Punkte zu kontrollieren und von allen Zentren, die auf die vertraulichen Informationen von CWT zugreifen, diese verwalten, speichern oder verarbeiten, zu trennen.

4.12 Die Rechenzentren des Anbieters müssen über Wärme-, Kühlungs-, Brandunterdrückungs-, Wasserdetektions- und Wärme-/Rauchdetektionsvorrichtungen verfügen.

5. Zugriffskontrolle

Der Anbieter verpflichtet sich zu Folgendem:

5.1 Alle vernünftigen Vorkehrungen zu treffen, um zu verhindern, dass Personen auf die vertraulichen Informationen von CWT in einer Weise oder zu einem Zweck, die bzw. der laut CWT und dem Vertrag nicht zulässig ist, Zugriff haben. Der Anbieter verpflichtet sich, den Zugang zu CWTs vertraulichen Informationen auf jene Dritte von ihm zu beschränken, die (1) ein legitimes Bedürfnis haben, auf die vertraulichen Informationen zuzugreifen, um gemäß dem Vertrag Dienstleistungen zu erbringen und die (2) schriftlich zugestimmt haben, die Integrität, Verfügbarkeit und Geheimhaltung der vertraulichen Informationen von CWT zu schützen.

5.2 Angemessene Verfahren zu unterhalten, um den Zugang zu CWTs vertraulichen Informationen, der Dritten des Anbieters gewährt wird, zu beenden, wenn dieser für die Erbringung ihrer Leistungen nicht länger notwendig bzw. relevant ist, sowie vor Beendigung der Beschäftigung oder Verpflichtung seitens CWT.

5.3 CWTs Informationen von sonstigen Anwendungen und Informationen von Kunden oder seinen eigenen zu trennen, indem er entweder physisch voneinander getrennte Server nutzt oder alternativ dazu überall dort logische Zugriffskontrollen einsetzt, wo es keine physische Trennung von Servern gibt.

5.4 Besitzer zu identifizieren und von diesen zu verlangen, den Zugang zu Systemen, über welche auf die vertraulichen Informationen von CWT zugegriffen wird, diese verarbeitet, verwaltet oder gespeichert werden, zu prüfen und zu genehmigen; ferner ist es die Aufgabe des Anbieters, die Zugangsgenehmigungen zu verwalten und zu beobachten.

5.5 Den Zugang zu Systemen, die zur Verwaltung personenbezogener Daten von CWT sowie geschützter Unternehmensdaten eingesetzt werden, binnen 24 Stunden, nachdem ein Mitarbeiter, Auftragnehmer, Unterauftragnehmer oder Dritter sein Verhältnis mit dem Anbieter beendet hat, aufzuheben; sowie binnen drei (3) Werktagen den Zugang zu jenen Systemen aufzuheben, wenn ein Mitarbeiter, Auftragnehmer, Unterauftragnehmer oder Dritter innerhalb des Unternehmens eine Arbeitsplatzänderung durchläuft. Alle sonstigen Nutzer-IDs sind nach 90 Kalendertagen der Inaktivität zu deaktivieren bzw. zu entfernen.

5.6 Regelmäßig, d. h. mindestens vierteljährlich, den Zugang zu Systemen, die zur Verwaltung personenbezogener Daten von CWT sowie geschützter Unternehmensdaten eingesetzt werden, zu überprüfen und Zugriffe zu genehmigen sowie ggf. unbefugte Zugriffe zu entfernen.

5.7 Den Zugriff auf CWTs vertrauliche Informationen ausschließlich auf befugte Mitarbeiter oder Systeme zu begrenzen sowie in Bezug auf seine eigenen Systeme und in Bezug auf die personenbezogenen Daten von CWT und geschützten Unternehmensdaten höchst restriktive Zugriffskontrollen einzusetzen.

5.8 Den Zugriff eines Systemadministrators (auch als Root-Benutzer, privilegierter Benutzer oder Superuser bekannt) auf Betriebssysteme, welche für die Verwendung durch mehrere Nutzer vorgesehen sind, ausschließlich auf jene Personen zu begrenzen, die zur Ausübung ihrer Arbeit einen derartigen Zugang auf höchster Ebene benötigen. In diesem Zusammenhang sind nach Möglichkeit IDs zur Abmeldung zusammen mit individuellen Benutzeranmeldeinformationen zur Verwaltung des Hochsicherheitszugangs einzusetzen; anderenfalls ist die Anzahl der Nutzer mit Zugang auf höchster Ebene extrem einzugrenzen.

5.9 Administratoren von Anwendungen, Datenbanken, Netzwerken und Systemen dazu aufzufordern, den Zugriff durch Nutzer ausschließlich auf jene Befehle, Daten, Systeme und sonstigen Ressourcen zu beschränken, welche diese zur Ausübung ihrer autorisierten Funktionen benötigen.

5.10 Bei Anwendung des Remotezugriffs eine starke Authentifizierung vorauszusetzen.

5.11 Angemessene technische und organisatorische Sicherheitsmaßnahmen einzusetzen, um zu verhindern, dass Dritte des Anbieters mit Zugriff auf personenbezogene Daten diese auf lokale Festplatten kopieren, verschieben oder speichern bzw. personenbezogene Daten ausschneiden und einfügen oder ausdrucken. Ein derartiges Vorgehen ist vom Anbieter zu verbieten.

5.12 Remotezugriffsfunktionen zu verwalten: die Anwendung der Remotezugriffsfunktionen nur bei Bedarf zu aktivieren, während der Anwendung zu überwachen und nach der Anwendung sofort wieder zu deaktivieren.

5.13 Mindestens eine Zwei-Faktor-Authentifizierung für Verbindungen zu internen Ressourcen des Anbieters, welche vertrauliche Informationen von CWT umfassen, vorauszusetzen.

6. Identifikation und Authentifizierung

Der Anbieter verpflichtet sich zu Folgendem:

6.1 Einzelnen Nutzern einmalige Nutzer-IDs zuzuweisen sowie Authentifizierungsmechanismen einem einzelnen Konto zuzuweisen.

6.2 Im Zusammenhang mit dem Lebenszyklus von Nutzer-IDs einen dokumentierten Verwaltungsprozess einzusetzen, einschließlich (jedoch nicht ausschließlich) Verfahren für die genehmigte Kontoerstellung, die rechtzeitige Kontoentfernung und Kontoanpassung (z. B. Änderungen der Berechtigungen, des Zugriffsbereichs, der Funktionen/Rollen), und zwar in Bezug auf den gesamten Zugang zu vertraulichen Informationen und das in allen Umgebungen (ob Produktion, Testumgebungen, Entwicklung usw.). Zu einem Verfahren dieser Art gehören außerdem die mindestens vierteljährlich stattfindende Überprüfung der Zugriffsrechte und der Kontogültigkeit.

6.3 Den Grundsatz der geringsten Berechtigungen durchzusetzen (d. h. den Zugriff ausschließlich auf jene Befehle, Informationen, Systeme und sonstigen Ressourcen zu beschränken, welche eine Person zur Ausübung ihrer autorisierten Funktionen gemäß ihrem Tätigkeitsbereich benötigt).

6.4 Vorauszusetzen, dass jeglicher Zugriff auf vertrauliche Informationen von CWT mittels einer gültigen Nutzer-ID und eines gültigen Passworts erfolgt und dass einmalige Nutzer-IDs die Voraussetzung für die Verwendung des Nachstehenden sind: Passwörter oder Passphrasen, Zwei-Faktor-Authentifizierung oder biometrische Werte.

6.5 Eine Passwortkomplexität vorauszusetzen, wobei die folgenden Bedingungen hinsichtlich des Passwortaufbaus erfüllt sein müssen: eine Mindestlänge von acht (8) Zeichen für Systempasswörter und von vier (4) Zeichen für Tablet- oder Smartphone-Passcodes. In Systempasswörter sind drei der nachstehenden Eigenschaften einzubauen: Großbuchstaben, Kleinbuchstaben, numerische Zeichen oder Sonderzeichen. Die Passwörter dürfen außerdem nicht mit der Nutzer-ID, zu dem sie gehören, identisch sein, ein Wort aus dem Wörterbuch, aufeinanderfolgende oder sich wiederholende Zahlen enthalten und nicht eines der letzten fünf Passwörter sein. Einen Ablauf von Passwörtern vorauszusetzen, und zwar in regelmäßigen Intervallen, die neunzig (90) Tage nicht überschreiten. Alle Passwörter bei Anzeige zu verbergen.

6.6 Die Anzahl fehlgeschlagener Anmeldeversuche auf maximal fünf (5) fehlgeschlagene Anmeldeversuche binnen 24 Stunden zu begrenzen und das Nutzerkonto nach Erreichen dieser Grenze dauerhaft zu sperren. Der Zugang zum Nutzerkonto kann anschließend per manuellem Verfahren, bei der die Verifizierung der Identität des Nutzers erforderlich ist, reaktiviert werden.

6.7 Die Identität des Nutzers zu verifizieren und für jeden einzelnen Nutzer Passwörter zum Einmalgebrauch und zum Zurücksetzen auf einen einmaligen Wert festzulegen. Nach der ersten Verwendung systematische Aufforderung zur Änderung.

6.8 Eine sichere Methode zur Übertragung der Anmeldeinformationen für die Authentifizierung (wie Passwörter) sowie sichere Mechanismen für die Authentifizierung (wie Tokens oder Smartcards) zu verwenden.

6.9 Für Dienstkonten- und Proxy-Passwörter eine Mindestlänge von 12 Zeichen festzulegen, darunter Großbuchstaben, Kleinbuchstaben, numerische Zeichen sowie Sonderzeichen. Mindestens jährlich die Dienstkonten- und Proxy-Passwörter zu ändern.

6.10 Interaktive Sitzungen zu beenden oder nach einer inaktiven Zeit von maximal fünfzehn (15) Minuten einen sicheren, sperrenden Bildschirmschoner mit Authentifizierungsaufforderung zu aktivieren.

6.11 Eine Authentifizierungsmethode zu wählen, welche auf der Sensibilität der vertraulichen Informationen von CWT beruht. Immer dann, wenn Anmeldeinformationen für die Authentifizierung gespeichert werden, verpflichtet sich der Anbieter, diese mittels starker Verschlüsselung zu schützen.

6.12 Systeme so zu konfigurieren, dass bei diesen nach einer maximalen Inaktivitätsphase automatisch die Zeitbegrenzung ausgelöst wird: Server (15 Minuten), Arbeitsplatz (15 Minuten), mobiles Gerät (4 Stunden), Dynamic Host Configuration Protocol (7 Tage), Virtual Private Network (24 Stunden).

7. Anschaffung, Entwicklung und Wartung von Informationssystemen

Der Anbieter verpflichtet sich zu Folgendem:

7.1 In Bezug auf durch CWT markengeschützte Produkte bzw. Dienstleistungen und Produkte oder in Bezug auf Software, welche für CWT entwickelt wird, auf Anmeldebildschirmen oder -seiten einen Hinweisbanner, wie schriftlich durch CWT vorgegeben, einzublenden.

7.2 Dafür Sorge zu tragen, dass alle Mitarbeiter, Unterauftragnehmer oder Beauftragte, welche Leistungen gemäß dem Vertrag erbringen, sich an die hier dargelegten technischen und organisatorischen Sicherheitsmaßnahmen halten; nachgewiesen mittels einer Vereinbarung, die mindestens genauso restriktiv wie die vorliegenden Informationssicherheitsanforderungen ist.

7.3 Alle Zugangsgeräte von CWT bzw. die CWT zur Verfügung stellt, so bald wie möglich, in jedem Fall jedoch spätestens fünfzehn (15) Tage, nachdem eines der nachstehenden Ereignisse als erstes eintritt, zurückzugeben:

(a) Ablauf oder Beendigung des Vertrags;
(b) CWTs Aufforderung zur Rückgabe der Gegenstände;
(c) der Tag, an dem der Anbieter die Geräte nicht mehr benötigt.

7.4 Eine effektive Methode zur Anwendungsverwaltung einzusetzen, bei der Informationen zu technischen und organisatorischen Sicherheitsmaßnahmen in den Softwareentwicklungsprozess einfließen, sowie sicherzustellen, dass die Informationen zu technischen und organisatorischen Sicherheitsmaßnahmen, wie in dem Softwareentwicklungslebenszyklus oder den Richtlinien zur Informationssicherheit bzw. den Standards und Verfahren von CWT dargelegt, vom Anbieter zeitnah umgesetzt werden.

7.5 Standardentwicklungsverfahren zu verfolgen, einschließlich der Trennung von Zugriff und Code zwischen Nichtproduktions- und Produktionsumgebungen und der damit verbundenen Aufgabentrennung zwischen diesen Umgebungen.

7.6 Sicherzustellen, dass interne Informationssicherheitskontrollen zur Softwareentwicklung in regelmäßigen Abständen bewertet werden und die Best Practices der Branche wiedergeben; diese Kontrollen zu korrigieren und rechtzeitig zu implementieren.

7.7 Die Sicherheit des Entwicklungsprozesses zu verwalten und dafür Sorge zu tragen, dass sichere Kodierungsverfahren implementiert sind und befolgt werden, darunter angemessene kryptografische Kontrollen, Schutzmaßnahmen vor schädlichen Codes sowie ein Peer-Review-Verfahren.

7.8 Penetrationstests bei funktionell vollständigen Anwendungen durchzuführen bzw. deren Durchführung zu veranlassen, und zwar mindestens einmal im Jahr sowie nach wesentlichen Änderungen am Quellcode oder der Konfiguration, die im Einklang mit OWASP, CERT, SANS Top 25 und PCI-DSS erfolgen. Ausnutzbare Schwachstellen vor Bereitstellung in der Produktionsumgebung zu korrigieren.

7.9 Anonymisierte oder entstellte Daten in Nichtproduktionsumgebungen zu verwenden. Unter keinen Umständen Produktionsdaten als Klartext in einer Nichtproduktionsumgebung zu verwenden sowie unter keinen Umständen personenbezogene Daten in Nichtproduktionsumgebungen aus welchem Grund auch immer zu verwenden. Dafür Sorge zu tragen, dass alle Testdaten und Testkonten vor Produktionsfreigabe entfernt werden.

7.10 Dafür Sorge zu tragen, dass Anbieter, die mit offenen Quellcodes, offener Software, offenen Anwendungen oder offenen Diensten arbeiten, diese sorgfältig prüfen, indem sie den erzeugten Code auf Fehler, Schwachstellen oder Sicherheitsprobleme, welche sich ggf. negativ auf die Datenintegrität, -verfügbarkeit oder -vertraulichkeit von CWT bzw. von CWTs Kunden auswirken, prüfen.

7.11 Dafür Sorge zu tragen, dass Anbieter unter keinen Umständen Codes, die im Rahmen des Vertrags erstellt werden, in gemeinsamen oder nichtprivaten Umgebungen, wie beispielsweise einem Code-Repository mit offenem Zugriff, unabhängig von der Entwicklungsstufe und unabhängig vom Kennwortschutz, mit anderen teilt.

8. Software- und Datenintegrität

Der Anbieter verpflichtet sich zu Folgendem:

8.1 In Umgebungen, für die eine Antivirensoftware im Handel erhältlich ist, eine aktuelle Antivirensoftware zu installieren und die Systeme nach Viren oder sonstiger Malware abzusuchen und diese von den Systemen oder Geräten umgehend zu entfernen oder in die Quarantäne zu verschieben.

8.2 Nichtproduktionsinformationen und -ressourcen von Produktionsinformationen und -ressourcen zu trennen.

8.3 Dafür Sorge zu tragen, dass die Teams in Bezug auf Systemänderungen einen dokumentierten Änderungskontrollprozess anwenden, einschließlich Back-out-Verfahren für alle Produktionsumgebungen sowie Notfalländerungsprozesse. Weiterhin ist sicherzustellen, dass alle Systemänderungen Tests, einer Dokumentation und einer Genehmigung unterliegen und dass wesentliche Änderungen in Bezug auf die genannten Prozesse der Genehmigung durch die Geschäftsführung unterliegen.

8.4 Soweit der Anbieter Daten von Karteninhabern verarbeitet oder speichert, verpflichtet sich dieser, eine PCI-Zone aufzubauen und aufrechtzuerhalten.

8.5 Für Anwendungen, bei denen eine Datenbank eingesetzt wird, die das Ändern vertraulicher Informationen von CWT zulässt, ist sicherzustellen, dass die Funktionen im Zusammenhang mit der

Überwachungsprotokollierung der Datenbanktransaktionen aktiviert sind und dass diese Überwachungsprotokolle für einen Zeitraum von mindestens sechs (6) Monaten aufbewahrt werden.

8.6 Soweit technisch realisierbar, sämtliche Software, die im Rahmen des Vertrags eingesetzt, zur Verfügung gestellt oder unterstützt wird, zu überprüfen, um während der Erstimplementierung oder nach wesentlichen Änderungen oder Aktualisierungen nach Sicherheitsschwachstellen zu suchen und diese zu beheben.

8.7 In Bezug auf Sicherheitskomponenten Tests zur Qualitätssicherung durchzuführen (Überprüfen der Identifikations-, Authentifizierungs- und Autorisierungsfunktionen) sowie sonstige Aktivitäten einzuleiten, die dafür ausgelegt sind, die Sicherheitsarchitektur zu überprüfen – während der Erstimplementierung oder nach wesentlichen Änderungen oder Aktualisierungen.

9. Systemsicherheit

Der Anbieter verpflichtet sich zu Folgendem:

9.1 In regelmäßigen Abständen die aktuellsten Versionen von Datenfluss- und Systemdiagrammen, welche für den Zugriff, die Verarbeitung, Verwaltung oder Speicherung von CWTs vertraulichen Informationen verwendet werden, zu erstellen bzw. zu aktualisieren.

9.2 Die Ressourcen der Branche (z. B., www.cert.org und einschlägige Mailinglisten und Websites von Softwareanbietern) aktiv zu beobachten, um rechtzeitig über relevante Sicherheitshinweise, die sich auf die Systeme des Anbieters oder sonstige Informationsressourcen beziehen, informiert zu sein.

9.3 Kryptografische Schlüssel effektiv zu verwalten, indem der Zugriff auf die Schlüssel auf die kleinste Anzahl erforderlicher Verwalter reduziert wird, geheime und private kryptografische Schlüssel mittels Verschlüsselung per Schlüssel, der mindestens genauso stark wie der datenverschlüsselnde Schlüssel ist, gespeichert werden und der getrennt von dem datenverschlüsselnden Schlüssel in einem sicheren kryptografischen System an so wenigen Orten wie möglich aufbewahrt wird. Änderung der kryptografischen Schlüssel von Default bei Installation sowie mindestens alle zwei Jahre; sichere Entsorgung der alten Schlüssel.

9.4 Mindestens vierteljährlich sowie vor Freigabe für Anwendungen und für wesentliche Änderungen und Aktualisierungen binnen Zeitfenstern infolge von Risikoanalysen, welche auf angemessenen und allgemein anerkannten IT-Richtlinien und IT-Standards beruhen, nach außen gerichtete Systeme und sonstige Informationsquellen, darunter u. a. Netzwerke, Server und Anwendungen, mit einer entsprechenden branchenüblichen Scansoftware zur Identifizierung von Sicherheitsschwachstellen abzusuchen, um etwaige Sicherheitsschwachstellen zu entdecken.

9.5 Mindestens vierteljährlich sowie vor Freigabe für Anwendungen und für wesentliche Änderungen und Aktualisierungen binnen Zeitfenstern infolge von Risikoanalysen, welche auf angemessenen und allgemein anerkannten IT-Richtlinien und IT-Standards beruhen, interne Systeme und sonstige Informationsquellen, darunter u. a. Netzwerke, Server, Anwendungen und Datenbanken mit einer entsprechenden branchenüblichen Scansoftware zur Identifizierung von Sicherheitsschwachstellen abzusuchen, um etwaige Sicherheitsschwachstellen zu entdecken; sicherzustellen, dass diese Systeme und sonstigen Ressourcen ordentlich gehärtet sind, darüber hinaus Identifizierung unbefugter drahtloser Netzwerke.

9.6 Im Hinblick auf die Ergebnisse der Schwachstellenanalyse ein Risikoeinstufungsverfahren zu unterhalten, basierend auf den Best Practices der Branche und der möglichen Auswirkung. Alle

Analyseergebnisse mit einem CVSS-Score von 4 oder höher sind per wiederholbarem Prozess handzuhaben.

9.7 Dafür Sorge zu tragen, dass alle seine Systeme und sonstigen Ressourcen „gehärtet“ sind und dies auch bleiben, einschließlich der Entfernung bzw. Deaktivierung nicht genutzter Netzwerke und sonstiger Dienste und Produkte (z. B. Finger-, Rlogin-, FTP- sowie einfache TCP/IP-Dienste und -Produkte) und eine Systemfirewall, Transmission-Control-Protocol -Wrapper (TCP-Wrapper) oder eine ähnliche Technologie zu installieren.

9.8 In Umgebungen, für die eine solche Technologie im Handel erhältlich ist und soweit diese zweckmäßig ist, eine oder mehrere Intrusion-Detection-Systeme (IDS), Intrusion-Prevention-Systeme (IPS) oder Intrusion-Detection-and-Prevention-Systeme (IDP) in einem aktiven Betriebsmodus bereitzustellen, um mit dessen/deren Unterstützung sämtlichen Traffic, der in Verbindung mit dem Vertrag in die Systeme und sonstigen Ressourcen ein- und wieder ausfließt, zu überwachen.

9.9 Über einen Risikoeinstufungsprozess zur Abhilfe von Sicherheitsschwachstellen in einem beliebigen System oder einer sonstigen Ressource zu verfügen, einschließlich (jedoch nicht ausschließlich) solcher Schwachstellen, die mittels Branchenpublikationen, Schwachstellenprüfung, Virenprüfung sowie mittels der Überprüfung von Sicherheitsprotokollen entdeckt werden; entsprechende Sicherheitspatches umgehend anzuwenden, unter Berücksichtigung der Wahrscheinlichkeit, dass eine solche Schwachstelle gerade ausgenutzt wird oder ausgenutzt werden kann. Kritische Patches bei einem CVSS-Score von 7,5 oder höher sind sofort bei Verfügbarkeit zu installieren und dürfen in keinem Fall später als einen Monat nach Veröffentlichung installiert werden. Kritische Patches bei einem CVSS-Score von 4 oder höher müssen binnen 90 Tagen nach Veröffentlichung installiert werden.

9.10 Mindestens jährlich sowie nach wesentlichen Upgrades oder Änderungen von Infrastrukturen oder Anwendungen intern und extern generalisierte Penetrationstests durchzuführen.

9.11 Nicht autorisierte Software, welche auf den Systemen des Anbieters entdeckt wird, zu entfernen oder zu deaktivieren sowie angemessene Malware-Kontrollen einzusetzen, darunter die Installation, regelmäßige Aktualisierung und routinemäßige Anwendung von Softwareprodukten gegen Malware, und zwar auf allen Diensten, Systemen und Geräten, über die auf die vertraulichen Informationen von CWT zugegriffen werden kann. Überall dort Antivirensoftware, die verlässlich ist und auf den Best Practices der Branche basiert, einzusetzen, wo es realisierbar ist, sowie sicherzustellen, dass die Virus-Definitionen stets aktuell sind.

9.12 Auf allen Diensten, Systemen und Geräten, über die auf vertrauliche Informationen von CWT zugegriffen werden kann, für eine ausreichend aktuelle Software zu sorgen, darunter die angemessene Wartung vom/von Betriebssystem(en) sowie die erfolgreiche Installation ausreichend aktueller Sicherheitspatches.

9.13 Konkreten Personen Aufgaben im Zusammenhang mit der Sicherheitsverwaltung zwecks Konfigurierung von Host-Betriebssystemen zuzuweisen.

9.14 Alle Standardkontonamen und/oder Standardpasswörter zu ändern.

10. Überwachung

Der Anbieter verpflichtet sich zu Folgendem:

10.1 Sofern nicht anders in diesem Vertrag angegeben, Protokolldaten zu CWTs vertraulichen Informationen für einen Zeitraum von mindestens 12 Monaten aufzubewahren und dafür Sorge zu tragen, dass diese Daten CWT binnen einer angemessenen Frist und auf Anfrage zur Verfügung gestellt werden.

10.2 Die primären Systemaktivitäten durch Dritte des Anbieters hinsichtlich Systemen, auf denen sich personenbezogene Daten von CWT sowie geschützte Unternehmensdaten befinden, aufzuzeichnen.

10.3 Den Zugriff auf Sicherheitsprotokolle auf befugte Personen zu begrenzen und die Sicherheitsprotokolle vor unbefugten Änderungen zu schützen.

10.4 Einen Mechanismus zur Änderungserkennung zu implementieren (z. B. Überwachung der Dateiintegrität), um Mitarbeiter auf unbefugte Änderungen von kritischen System-, Konfigurations- oder Inhaltsdateien aufmerksam zu machen; Software so zu konfigurieren, dass diese wöchentlich kritische Dateivergleiche durchführt.

10.5 Mindestens einmal pro Woche alle Sicherheits- und sicherheitsrelevanten Überwachungsprotokolle auf Systemen, auf denen sich personenbezogene Daten von CWT sowie geschützte Unternehmensdaten befinden, auf Abweichungen hin zu überprüfen und alle protokollierten Sicherheitsprobleme zeitnah zu dokumentieren und zu beheben.

10.6 Täglich alle Sicherheitsereignisse, Protokolle von Systemkomponenten, über die Daten von Karteninhabern gespeichert, verarbeitet oder übertragen werden, Protokolle von kritischen Systemkomponenten sowie Protokolle von Server- und Systemkomponenten mit Sicherheitsfunktionen zu überprüfen.

11. Sicherheitsgateways

Der Anbieter verpflichtet sich zu Folgendem:

11.1 Für den Administrator- und/oder Verwaltungszugriff auf Sicherheitsgateways eine starke Authentifizierung vorauszusetzen, darunter u. a. der Zugang zwecks Überprüfung der Protokolldateien.

11.2 Über dokumentierte Kontrollen, Richtlinien, Prozesse und Verfahren zu verfügen und diese anzuwenden, damit sichergestellt ist, dass unbefugte Nutzer keinen Administrator- und/oder Verwaltungszugriff auf Sicherheitsgateways haben und dass die Berechtigungsstufen von Nutzern zwecks Administration und Verwaltung der Sicherheitsgateways angemessen sind.

11.3 Mindestens einmal in sechs (6) Monaten zu überprüfen, dass die Konfigurationen von Sicherheitsgateways gehärtet sind; hierzu sind stichprobenartig Sicherheitsgateways auszuwählen, wobei dann jeder Standardregelsatz und jeder Konfigurationsparametersatz auf die nachstehenden Einstellungen hin zu überprüfen ist:

a. Quellrouting des Internetprotokolls (IP) ist deaktiviert;
b. Die Loopback-Adresse hat keinen Zugang zum internen Netzwerk;
c. Anti-Spoofing-Filter sind implementiert;
d. Broadcast-Paketen ist der Zugang zum Netzwerk verwehrt;
e. Internet-Control-Message-Protocol-Umleitungen (ICMP-Umleitungen) sind deaktiviert;
f. Alle Regelsätze enden mit einer „DENY ALL“-Anweisung;
g. Jede Regel ist auf eine konkrete Geschäftsanfrage rückführbar.

11.4 Dafür Sorge zu tragen, dass Überwachungstools eingesetzt werden, um zu überprüfen, dass alle Aspekte von Sicherheitsgateways (wie Hardware, Firmware und Software) permanent betriebsbereit sind.

Dafür Sorge zu tragen, dass alle Sicherheitsgateways so konfiguriert und implementiert sind, dass alle nicht betriebsbereiten Sicherheitsgateways den gesamten Zugang verweigern.

11.5 Eingehende Pakete von einem nicht vertrauenswürdigen externen Netzwerk dürfen die DMZ nicht übertreten und es darf ihnen nicht gestattet werden, direkt zum vertrauenswürdigen internen Netzwerk vorzudringen. Alle eingehenden Pakete, die zum vertrauenswürdigen internen Netzwerk vordringen, müssen ihren Ursprung in der DMZ haben. Die DMZ ist mittels eines Sicherheitsgateways vom nicht vertrauenswürdigen externen Netzwerk zu trennen und darüber hinaus wie folgt vom vertrauenswürdigen internen Netzwerk zu trennen:

a. mittels eines weiteren Sicherheitsgateways, oder
b. mittels desselben Sicherheitsgateways, das eingesetzt wird, um die DMZ von dem nicht vertrauenswürdigen externen Netzwerk zu trennen, wobei sichergestellt sein muss, dass durch das Sicherheitsgateway Pakete, die aus dem nicht vertrauenswürdigen externen Netzwerk eingehen, entweder sofort gelöscht werden, oder, sollte eine Löschung nicht stattfinden, lediglich an die DMZ weitergeleitet werden, ohne dass dabei eine weitere Verarbeitung dieser eingehenden Pakete stattfindet, mit Ausnahme einer möglichen Aufzeichnung der Pakete in einer Logdatei.

Die folgenden Informationen dürfen sich ausschließlich innerhalb des vertrauenswürdigen internen Netzwerkes befinden:

a. Personenbezogene Daten von CWT oder geschützte Unternehmensdaten, die ohne starke Verschlüsselung gespeichert werden;
b. Die offizielle Datensatzkopie von Informationen, auf die per Anfragen, die von dem nicht vertrauenswürdigen externen Netzwerk ausgehen, zugegriffen werden soll;
c. Die offizielle Datensatzkopie von Informationen, die infolge von Anfragen, die von dem nicht vertrauenswürdigen externen Netzwerk ausgehen, geändert werden sollen;
d. Datenbankserver;
e. Alle exportierten Protokolle;
f. Alle Umgebungen, welche zwecks Entwicklung, Tests, Sandkasten, Produktion eingesetzt werden und alle sonstigen derartigen Umgebungen, sowie alle Quellcodeversionen.

11.6 Anmeldeinformationen für die Authentifizierung, die nicht mittels starker Verschlüsselung geschützt sind, dürfen sich nicht innerhalb der DMZ befinden.

12. Netzwerksicherheit

Der Anbieter verpflichtet sich zu Folgendem:

12.1 Auf Anfrage von CWT diesem ein logisches Netzwerkdiagramm zur Verfügung zu stellen, auf dem Systeme und Verknüpfungen zu anderen Ressourcen, darunter Router, Switches, Firewalls, IDS-Systeme, Netzwerktopologie, externe Verbindungsstellen, Gateways, drahtlose Netzwerke und sonstige CWT unterstützende Geräte, dokumentiert sind.

12.2 Einen formalen Prozess zur Genehmigung, Testung und Dokumentation aller Netzwerkverbindungen sowie aller Änderungen in Bezug auf Firewall- und Routerkonfigurationen zu unterhalten. Firewalls so zu konfigurieren, dass diese verdächtigen Paketen den Zugang verwehren und diese

protokollieren, und lediglich jenen Traffic zu erlauben, der zulässig und autorisiert ist, und allen anderen Traffic den Zugang durch die Firewall zu verwehren. Die Firewall-Regeln alle sechs Monate zu überprüfen.

12.3 An jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone eine Firewall zu installieren. Jedes System, auf dem personenbezogene Daten gespeichert werden, muss sich innerhalb der internen Netzwerkzone befinden, getrennt von der DMZ und anderen vertrauenswürdigen Netzwerken.

12.4 Bei Bedarf Firewalls am Rand und innen zu überwachen.

12.5 Über einen dokumentierten Prozess sowie Kontrollen zu verfügen, um nicht autorisierte Zugriffsversuche auf die vertraulichen Informationen von CWT zu entdecken und abzuwickeln.

12.6 Bei Bereitstellung internetbasierter Dienste und Produkte gegenüber CWT: die vertraulichen Informationen von CWT durch Implementierung einer DMZ im Netzwerk zu schützen. Webserver, über die Dienste für CWT erbracht werden, müssen sich innerhalb der DMZ befinden. Jedes System und jede Informationsressource, auf denen CWTs vertrauliche Informationen gespeichert werden (wie Anwendungs- und Datenbankserver), müssen sich in einem vertrauenswürdigen internen Netzwerk befinden. (Bei Internetdiensten und -produkten ist eine DMZ sicherzustellen).

12.7 Den nicht autorisierten ausgehenden Traffic von Anwendungen, die innerhalb der DMZ und des Internets vertrauliche Informationen verarbeiten, speichern oder an IP-Adressen übertragen, zu begrenzen.

12.8 Bei Verwendung von auf Hochfrequenz basierenden drahtlosen Netzwerktechnologien, um Dienste und Produkte für CWT zu erbringen bzw. zu unterstützen, sorgt der Anbieter dafür, dass sämtliche vertrauliche Informationen von CWT, die übertragen werden, mittels entsprechender Verschlüsselungstechnologien, welche ausreichend sind, um die Geheimhaltung der vertrauliche Informationen von CWT aufrechtzuerhalten, geschützt werden; dies gilt in jedem Fall unter der Voraussetzung, dass für eine solche Verschlüsselung Schlüssellängen von mindestens 256 Bits für die symmetrische Verschlüsselung bzw. 1024 Bits für die asymmetrische Verschlüsselung eingesetzt werden. Ferner wird der Anbieter in regelmäßigen Abständen nach nicht autorisierten drahtlosen Zugriffspunkten suchen, diese identifizieren und deaktivieren.

13. <u>Konnektivitätsanforderungen</u>

13.1 Für den Fall, dass der Anbieter zu den vertraulichen Informationsressourcen von CWT in Verbindung mit dem Vertrag über Konnektivität verfügt bzw. diese ihm bereitgestellt werden soll, verpflichtet sich der Anbieter neben dem Vorstehendem zu Folgendem:

a. Ausschließlich die gemeinsam vereinbarten Einrichtungen und Verbindungsmethoden zu nutzen, um die vertraulichen Informationsressourcen von CWT mit seinen eigenen Ressourcen zu verbinden.
b. Ohne die vorherige Zustimmung von CWT KEINE Vernetzung zu den vertraulichen Informationsressourcen von CWT aufzubauen.
c. CWT während der normalen Geschäftszeiten Zugang zu den entsprechenden Einrichtungen des Anbieters zwecks Wartung und Support von Geräten (wie bspw. Routern), die von CWT im Rahmen des Vertrags zwecks Konnektivität zu den vertraulichen Informationsressourcen von CWT bereitgestellt werden, zu gewähren.
d. Die von CWT im Rahmen des Vertrags zwecks Konnektivität zu den vertraulichen Informationsressourcen von CWT zur Verfügung gestellten Geräte ausschließlich zur

Erbringung/Bereitstellung jener Dienste und Produkte oder Funktionen, wie im Vertrag ausdrücklich befugt, zu nutzen.

e. Sollte es für die vereinbarte Konnektivitätsmethode erforderlich sein, dass der Anbieter ein Sicherheitsgateway implementiert, sind zu allen Sitzungen, bei denen dieser Sicherheitsgateway zum Einsatz kommt, Protokolle zu führen. In diesen Sitzungsprotokollen müssen ausreichend detaillierte Informationen enthalten sein, anhand derer der Endnutzer oder die Endanwendung, die Quell-IP-Adresse, Ziel-IP-Adresse, die verwendeten Ports/Serviceprotokolle und die Dauer des Zugriffs ermittelbar sind. Die Sitzungsprotokolle sind ab Sitzungserstellung für einen Zeitraum von mindestens sechs (6) Monaten aufzubewahren.

13.2 Für den Fall, dass der Anbieter zu den vertraulichen Informationsressourcen von CWT in Verbindung mit dem Vertrag über Konnektivität verfügt bzw. diese ihm bereitgestellt werden soll, erlaubt der Anbieter CWT – neben den anderen in diesem Dokument festgehaltenen Rechten – Folgendes:

a. Informationen in Verbindung mit dem Zugang, einschließlich den des Anbieters, zu den vertraulichen Informationsressourcen von CWT zu sammeln. Diese Informationen können ohne weitere Benachrichtigung von CWT zwecks Identifizierung möglicher Sicherheitsrisiken erfasst, aufbewahrt und analysiert werden. Zu diesen Informationen können zählen: Tracedateien, Statistiken, Netzwerkadressen sowie die tatsächlichen Daten oder Bildschirme, auf die zugegriffen wird bzw. die übertragen werden.
b. Verbindungen zu vertraulichen Informationsressourcen von CWT sofort zu unterbrechen oder zu beenden, wenn nach Auffassung (und alleinigem Ermessen) von CWT ein Sicherheitsverstoß vorliegt oder es in Verbindung mit den Dateneinrichtungen von CWT, den Informationen von CWT, Systemen oder sonstigen Ressourcen zu einem unbefugten Zugriff oder einer missbräuchlichen Verwendung gekommen ist.

14. Mobile und tragbare Geräte

Der Anbieter verpflichtet sich zu Folgendem:

14.1 Zum Schutz der vertraulichen Informationen von CWT, welche auf mobilen und tragbaren Geräten abgelegt sind, eine starke Verschlüsselung zu nutzen.

14.2 Keine personenbezogenen Daten auf mobilen Geräten oder Laptops zu speichern und keine personenbezogenen Daten von CWT sowie geschützte Unternehmensdaten auf Wechseldatenträgern zu speichern, sofern er hierbei nicht eine starke Verschlüsselung nutzt.

14.3 Zum Schutz der vertraulichen Informationen von CWT, die übertragen werden, eine starke Verschlüsselung zu nutzen – unter Verwendung von bzw. durch Remotezugriff per netzwerksensibler mobiler und tragbarer Geräte.

a. Bei der Verwendung netzwerksensibler mobiler und tragbarer Geräte, bei denen es sich nicht um Laptops handelt, um auf vertrauliche Informationen von CWT zuzugreifen und/oder um diese zu speichern, müssen diese Geräte in der Lage sein, alle abgespeicherten Kopien der vertraulichen Informationen von CWT nach Eingang eines ordnungsgemäß authentifizierten Befehls über das Netzwerk zu löschen (Hinweis: Diese Funktion wird oft auch als „Remote Wipe“ bezeichnet).
b. Es muss dokumentierte Richtlinien, Verfahren und Standards geben, mit denen sichergestellt wird, dass die autorisierte Person, unter deren physischer Kontrolle ein netzwerksensibles mobiles und tragbares Gerät, bei dem es sich nicht um einen Laptop handelt und auf dem vertrauliche Informationen von CWT abspeichert sind, unverzüglich die Löschung sämtlicher vertraulicher Informationen von CWT in die Wege leitet, wenn das Gerät verloren geht oder gestohlen wird.

c. Es muss dokumentierte Richtlinien, Verfahren und Standards geben, wonach mobile und tragbare Geräte, bei denen es sich nicht um Laptops handelt und die nicht netzwerksensibel sind, automatisch alle gespeicherten Kopien der vertraulichen Informationen von CWT löschen, nachdem es zu mehreren aufeinanderfolgenden Fehlversuchen bei der Anmeldung gekommen ist.

14.4 Über dokumentierte Richtlinien, Verfahren und Standards zu verfügen, mit denen sichergestellt wird, dass alle mobilen und tragbaren Geräte, die für den Zugriff auf und/oder der Speicherung von CWTs vertraulichen Informationen genutzt werden:

a. sich im physischen Besitz autorisierter Personen befinden;
b. physisch abgesichert sind, sofern sie sich nicht im physischen Besitz autorisierter Personen befinden; oder
c. es ist sichergestellt, dass deren Datenspeicher sofort und auf sichere Weise gelöscht wird, sofern sich die Geräte weder im physischen Besitz autorisierter Personen befinden, noch physisch abgesichert sind oder es zu 10 fehlgeschlagenen Anmeldeversuchen gekommen ist.

14.5 Bevor der Zugriff auf CWTs vertrauliche Informationen erlaubt wird, welche auf mobilen und tragbaren Geräten abgespeichert sind oder über diese abgespeichert werden, muss der Anbieter über einen Prozess verfügen und diesen anwenden, mit dem sichergestellt wird, dass:

a. der Nutzer für einen solchen Zugriff die Befugnis hat; und
b. die Identität des Nutzers authentifiziert wurde.

14.6 Eine Richtlinie einzuführen, wonach die Verwendung mobiler und tragbarer Geräte, die nicht vom Anbieter oder CWT verwaltet werden, zwecks des Zugriffs auf und/oder der Speicherung der vertraulichen Informationen von CWT verboten ist.

14.7 Mindestens einmal im Jahr die Verwendung von sämtlichen mobilen und tragbaren Geräten, die vom Anbieter verwaltetet werden, sowie die Kontrollen für diese zu überprüfen, um sicherzustellen, dass die mobilen und tragbaren Geräte in der Lage sind, die technischen und organisatorischen Sicherheitsmaßnahmen zu erfüllen.

15. Sicherheit in Transitumgebungen

Der Anbieter verpflichtet sich zu Folgendem:

15.1 Für die Übertragung von CWTs vertraulichen Informationen außerhalb von Netzwerken, die weder von CWT noch dem Anbieter kontrolliert werden, bzw. in Fällen, in denen CWTs vertrauliche Informationen über ein nicht vertrauenswürdiges Netzwerk übertragen werden, eine starke Verschlüsselung zu nutzen.

15.2 Aufzeichnungen mit personenbezogenen Daten von CWT und geschützten Unternehmensdaten in Papierformat, auf Mikrofiche oder elektronischen Medien, welche physisch übertragen werden, müssen mittels eines sicheren Kurierdienstes oder einer sonstigen Liefermethode transportiert werden, die nachverfolgbar ist und bei der alles sicher und nach den Vorgaben des Herstellers verpackt ist. Personenbezogene Daten von CWT und geschützte Unternehmensdaten sind in verschlossenen Behältnissen zu transportieren.

16. Sicherheit in stationären Umgebungen

16.1 Der Anbieter verpflichtet sich, bei der Speicherung personenbezogener Daten von CWT und geschützter Unternehmensdaten eine starke Verschlüsselung zu nutzen.

16.2 Der Anbieter verpflichtet sich, keine personenbezogenen Daten von CWT und keine geschützten Unternehmensdaten außerhalb der eigenen Netzwerkumgebung (oder außerhalb CWTs sicherem Computernetzwerk) elektronisch zu speichern, sofern die Speichervorrichtung (wie Sicherungsband, Laptop, Speicherstick, Diskette usw.) nicht per starker Verschlüsselung geschützt ist.

16.3 Der Anbieter verpflichtet sich, keine personenbezogenen Daten von CWT und keine geschützten Unternehmensdaten auf Wechseldatenträgern (wie USB-Flashlaufwerken, Speichersticks, Bändern, CDs oder externen Festplatten) zu speichern, außer: (a) zwecks Backup, Geschäftskontinuität, Notfallwiederherstellung oder Datenaustausch, wie gemäß Vertrag erlaubt und erforderlich und (b) unter Verwendung einer starken Verschlüsselung.

16.4 Der Anbieter verpflichtet sich, Aufzeichnungen mit personenbezogenen Daten von CWT und geschützten Unternehmensdaten in Papierformat oder auf Mikrofiche in Bereichen aufzubewahren und zu sichern, zu denen ausschließlich befugte Personen Zutritt haben.

16.5 Sofern nicht anderweitig schriftlich von CWT angewiesen, verpflichtet sich der Anbieter bei der Erfassung, Erzeugung oder Erstellung von vertraulichen Informationen in Papierform oder als Sicherungsmedien für, durch oder im Auftrag von CWT bzw. unter der Marke CWT, diese Informationen als zu CWT zugehörige vertrauliche Informationen kenntlich zu machen und, soweit durchführbar, diese Informationen von CWT als „Vertraulich“ oder „Geschützt“ zu kennzeichnen. Der Anbieter erkennt an, dass die vertraulichen Informationen von CWT in dessen Eigentum bleiben, unabhängig von der Kennzeichnung oder einem Fehlen derer.

17. Rückgabe, Vernichtung und Entsorgung

17.1 Der Anbieter verpflichtet sich, ohne zusätzliche Kosten für CWT und auf Anfrage von CWT, Kopien von CWTs vertraulichen Informationen an CWT binnen dreißig (30) Tagen nach einer solchen Anfrage zur Verfügung zu stellen. Er verpflichtet sich ebenfalls alle vertraulichen Informationen von CWT zurückzugeben oder auf Wunsch von CWT zu vernichten, darunter elektronische Kopien und Ausdrucke, und zwar binnen neunzig (90) Tagen, sobald eines der nachstehenden Ereignisse eintritt: Ablauf oder Beendigung des Vertrags, CWTs Aufforderung zur Rückgabe der vertraulichen Informationen von CWT, der Tag, an dem der Anbieter CWTs vertrauliche Informationen nicht länger zur Ausübung/Bereitstellung seiner Dienste oder Produkte gemäß Vertrag benötigt.

17.2 Für den Fall, dass CWT der Vernichtung als Alternative zur Rückgabe der vertraulichen Informationen von CWT zustimmt, bestätigt der Anbieter schriftlich die Vernichtung dieser vertraulichen Informationen und damit gleichzeitig, dass diese nicht länger abrufbar oder wiederherstellbar sind. Der Anbieter verpflichtet sich außerdem, alle Kopien der vertraulichen Informationen von CWT an allen Orten und in allen Systemen, an bzw. in denen die vertraulichen Informationen von CWT aufbewahrt/gespeichert sind, vollständig zu vernichten. Dies schließt u. a. auch im Vorfeld genehmigte Dritte des Anbieters ein. Die Informationen sind gemäß einem in der Branche üblichen Standardverfahren zur vollständigen Zerstörung zu vernichten, z. B. DOD 5220.22M oder die NIST-Sonderveröffentlichung 800-88 oder mittels einem vom Hersteller für das jeweilige System empfohlenen Produkts zur Entmagnetisierung. Vor einer derartigen Vernichtung verpflichtet sich der Anbieter zur Erhaltung aller anwendbaren technischen und organisatorischen Sicherheitsmaßnahmen, um die Sicherheit, Vertraulichkeit und Geheimhaltung der vertraulichen Informationen von CWT zu schützen.

17.3 Der Anbieter verpflichtet sich, personenbezogene Daten von CWT und geschützte Unternehmensdaten in einer Weise zu entsorgen, die gewährleistet, dass die Informationen nicht wieder in ein nutzbares Format zurückgeführt werden können. Blätter, Folien, Mikrofilme, Mikrofiches und Fotos sind zu schreddern oder zu verbrennen. Materialien, die personenbezogene Daten von CWT und geschützte Unternehmensdaten enthalten und vernichtet werden sollen, sind in abgesicherten Behältnissen zu lagern und der Transport ist über einen sicheren Dritten abzuwickeln.

18. Aufbewahrung

18.1 Für den Fall, dass der Anbieter Kopien der vertraulichen Informationen von CWT länger als neunzig (90) Tage nach Ablauf oder Beendigung des Vertrags bzw. nach Aufforderung durch CWT zur Rückgabe oder Vernichtung der vertraulichen Informationen von CWT aufbewahren muss, darf der Anbieter diese Kopien aufbewahren, wenn dies schriftlich mit CWT vereinbart wurde. Kopien der vertraulichen Informationen von CWT dürfen länger als neunzig (90) Tage nach Ablauf oder Beendigung des Vertrags aufbewahrt werden, ohne dass hierfür die schriftliche Zustimmung von CWT eingeholt werden muss, wenn eine solche längere Aufbewahrung zur Einhaltung gesetzlicher Vorgaben erforderlich ist.

18.2 In jedem Fall ist der Anbieter dafür verantwortlich, die entsprechenden Aufbewahrungsanforderungen von Kontakten bei CWT bestätigen zu lassen, und zwar bevor er in den Besitz von irgendwelchen vertraulichen Informationen von CWT kommt, sowie in Übereinstimmung mit etwaigen Leistungsbeschreibungen oder Aufträgen.

18.3 Der Anbieter verpflichtet sich zum Schutz etwaiger Sicherungskopien von CWTs vertraulichen Informationen, welche automatisch von seinen eigenen Diensten, Systemen, Geräten oder Medien bzw. denen von Dritten erstellt werden („**Archivkopien**"). Binnen 90 Kalendertagen nach Ablauf oder Beendigung des Vertrags bzw. früher, sofern in vernünftiger Weise von CWT gefordert, ist der Anbieter verpflichtet, alle Archivkopien von CWTs vertraulichen Informationen auf sichere Weise zu vernichten. Hierbei ist ein Standardverfahren anzuwenden, dass mindestens genauso restriktiv wie der DOD 5220.22M oder die NIST-Sonderveröffentlichung 800-88 ist.

19. Reaktion auf Störfälle und Benachrichtigung

Der Anbieter verpflichtet sich zu Folgendem:

19.1 Über einen Prozess für das Störfallmanagement und über dazugehörige Verfahren zu verfügen und diese anzuwenden sowie für diesen Prozess und diese Verfahren spezialisierte Mitarbeiter einzusetzen. Sofort und in jedem Fall innerhalb von vierundzwanzig (24) Stunden CWT über jegliche vermutete oder bestätigte Angriffe, Eindringversuche, unbefugte Zugriffe, Verlustvorfälle oder sonstige Störfälle in Bezug auf die Informationen, Systeme oder sonstigen Ressourcen von CWT zu informieren.

19.2 Nach der Benachrichtigung von CWT, CWT regelmäßige Statusupdates zur Verfügung zu stellen, darunter u. a. ergriffene Maßnahmen zur Behebung des Störfalls, und zwar in einvernehmlich vereinbarten Intervallen oder zu einvernehmlich vereinbarten Zeitpunkten für die Dauer des Störfalls und darüber hinaus so schnell wie vernünftigerweise möglich nach Beendigung des Störfalls CWT einen schriftlichen Bericht zukommen zu lassen, in dem der Störfall, die vom Anbieter während seiner Reaktion ergriffenen Maßnahmen und dessen Pläne für künftige Maßnahmen zur Abwendung ähnlicher Störfälle beschrieben sind.

19.3 Unter keinen Umständen ohne vorher CWT benachrichtigt zu haben, Verstöße hinsichtlich der Informationen, Systeme oder sonstigen Ressourcen von CWT öffentlich zu machen und darüber hinaus direkt mit CWT zusammenzuarbeiten, um die entsprechenden Regierungsvertreter auf lokaler, kommunaler, Landes- oder Bundesebene oder die von einem solchen Verstoß betroffenen Kreditüberwachungsdienste oder Personen zu informieren, einschließlich der entsprechenden Medienkanäle, wie dies gesetzlich vorgeschrieben ist.

a. Der Anbieter muss über einen Prozess verfügen, der es ermöglicht, dass Verstöße im Hinblick auf die Sicherheitskontrollen, einschließlich der in den vorliegenden Informationssicherheitsanforderungen beschriebenen, welche vom Personal des Anbieters ausgehen, unverzüglich erkannt werden. Die ermittelten Mitarbeiter sind dann unter Berücksichtigung der geltenden Gesetze entsprechenden Disziplinarmaßnahmen auszusetzen. Ungeachtet des Vorstehenden unterstehen die Mitarbeiter des Anbieters weiterhin diesem. CWT gilt nicht als Arbeitgeber der Mitarbeiter des Anbieters.

20. Betriebskontinuitätsmanagement und Notfallwiederherstellung

Der Anbieter verpflichtet sich zu Folgendem:

20.1 Pläne zur Business Continuity (Geschäftskontinuität) und IT- (Notfallwiederherstellung) zu entwickeln, zu betreiben, zu verwalten und zu verbessern, um die Auswirkungen für CWT im Hinblick auf die Dienste oder Produkte des Anbieters zu minimieren. Diese Pläne sollten enthalten: die Namen derer, welche konkret für die Business Continuity und Disaster Recovery verantwortlich sind; geltende Recovery Time Objectives und Recovery Point Objectives; tägliche Backups von Daten und Systemen; externe Lagerung von Sicherungsmedien und -datensätzen; Schutz der Datensätze und Notfallpläne in Übereinstimmung mit den Anforderungen des Vertrags. Diese Pläne sind an einem externen Ort sicher und in einer Weise aufzubewahren, dass der Anbieter auf diese im Bedarfsfall zugreifen kann.

20.2 CWT auf dessen Anfrage einen dokumentierten Plan zur Business Continuity vorzulegen, mit dem gewährleistet wird, dass der Anbieter seinen Vertragspflichten nachkommen kann, einschließlich etwaiger Pflichten aus Leistungsbeschreibungen oder Service-Level-Agreements. Mit den Plänen soll die Wiederherstellung bei gleichzeitiger Sicherung der Integrität und Geheimhaltung der vertraulichen Informationen von CWT gewährleistet werden.

20.3 Über dokumentierte Verfahren verfügen, um sichere Backups und eine sichere Wiederherstellung der vertraulichen Informationen von CWT zu gewährleisten; dazu sollten mindestens gehören: Verfahren zum Transport, der Lagerung und Entsorgung der Sicherungskopien von CWTs vertraulichen Informationen und, sofern dies CWT wünscht, diese dokumentierten Verfahren CWT zur Verfügung zu stellen.

20.4 Dafür Sorge zu tragen, dass Backups von sämtlichen vertraulichen Informationen von CWT, die gespeichert sind, oder von Software oder Konfigurationen für Systeme, welche von CWT genutzt werden, mindestens einmal pro Woche erstellt werden.

20.5 In regelmäßigen Abständen, jedoch mindestens jährlich, oder nach wesentlichen Änderungen der Pläne zur Business Continuity oder Disaster Recovery, diese Pläne auf eigene Kosten auf ihre Tauglichkeit hin prüfen. Auf diese Weise sollen die ordnungsgemäße Funktionsweise der betroffenen Technologien und die interne Kenntnis dieser Pläne sichergestellt werden.

20.6 Unverzüglich seinen Plan zur Business Continuity zu überarbeiten, um zusätzliche oder aufkommende Gefahrenquellen bzw. -szenarien zu berücksichtigen und darüber hinaus CWT auf

Anfrage innerhalb eines angemessenen Zeitrahmens eine überblicksartige Zusammenfassung der Pläne und Tests zur Verfügung zu stellen.

20.7 Dafür Sorge zu tragen, dass alle Standorte des Anbieters bzw. alle Standorte, mit denen er einen Vertrag abgeschlossen hat, in denen sich vertrauliche Informationen von CWT befinden bzw. in denen diese verarbeitet werden, rund um die Uhr und sieben (7) Tage die Woche überwacht werden, um diese vor Eindringlingen, Feuer, Wasser oder sonstigen Umweltgefahren zu schützen.

21. Einhaltung und Zulassungen

21.1 Der Anbieter verpflichtet sich, vollständige und akkurate Aufzeichnungen hinsichtlich der Erfüllung seiner Pflichten, welche sich aus den vorliegenden Informationssicherheitsanforderungen ergeben, beizubehalten und wird dies in einem Format tun, das Bewertungen oder Prüfungen für einen Zeitraum von mindestens drei (3) Jahren oder ggf. auch länger, wenn dies nach einem Gerichtsbeschluss, Zivil- oder Regulierungsverfahren erforderlich ist, ermöglicht. Ungeachtet des Vorstehenden ist der Anbieter verpflichtet, Sicherheitsprotokolle für einen Zeitraum von mindestens sechs (6) Monaten nach einer weiteren Ausübung des vorliegenden Vertrags zu erhalten.

21.2 CWT kann, ohne zusätzliche Kosten für CWT und vorbehaltlich einer angemessenen Ankündigung im Voraus, regelmäßige Sicherheitsbewertungen oder -prüfungen der vom Anbieter angewandten technischen und organisatorischen Sicherheitsmaßnahmen durchführen, im Rahmen derer CWT dem Anbieter schriftliche Fragebögen und Anfragen zur Dokumentation zukommen lassen kann. Der Anbieter wird dann auf alle Anfragen schriftlich und, falls zutreffend, mit Nachweisen sofort reagieren bzw. in beiderseitigem Einverständnis, sofern ersteres im angemessenen Maß nicht möglich ist. Nachdem CWT um eine Prüfung angefragt hat, wird der Anbieter eine Sicherheitsprüfung organisieren, die binnen zehn (10) Geschäftstagen nach einer solchen Anfrage beginnt. CWT kann hierbei den Zugang zu Einrichtungen, Systemen, Prozessen oder Verfahren zwecks der Beurteilung der Sicherheitskontrollumgebung des Anbieters verlangen.

21.3 Auf Anfrage von CWT wird der Anbieter Nachweise zur Verfügung stellen, aus denen seine Einhaltung der Vertragsbestimmungen hervorgeht, einschließlich unterstützender Zertifizierungen hinsichtlich der aktuellsten Versionen des PCI-DSS, der ISO 27001/27002, SOC 2 oder ähnlichen Bewertungen zum Anbieter, zu Unterauftragnehmern oder Dritten, welche im Auftrag des Anbieters Informationen verarbeiten, speichern, verwalten oder auf diese zugreifen.

21.4 Für den Fall, dass CWT nach alleinigem Ermessen befindet, dass es zu einem Sicherheitsverstoß gekommen ist, der nicht unverzüglich in Übereinstimmung mit dem Störfallmanagement-Prozess des Anbieters CWT gemeldet wurde, verpflichtet sich der Anbieter, eine Prüfung oder Bewertung festzusetzen, die binnen vierundzwanzig (24) Stunden nach der Mitteilung durch CWT, in der eine Bewertung oder Prüfung gefordert wird, beginnt. Mit dieser Bestimmung werden keine strengeren Prüfungspflichten, wonach die Untersuchung der im Vertrag enthaltenen Aufzeichnungen des Anbieters erlaubt ist, begrenzt. Auch darf die Bestimmung auf diese Weise nicht ausgelegt werden.

21.5 Binnen dreißig (30) Kalendertagen nach Erhalt der Endergebnisse der Bewertung oder des Prüfberichts stellt der Anbieter CWT einen schriftlichen Bericht zur Verfügung, in dem die Abhilfemaßnahmen des Anbieters, die dieser bereits eingeführt hat bzw. plant einzuführen, dargelegt sind, zusammen mit dem Zeitplan und aktuellen Stand zu jeder einzelnen Abhilfemaßnahme. Der Anbieter wird diesen Bericht an CWT alle dreißig (30) Kalendertage aktualisieren und darin den Stand aller Abhilfemaßnahmen mittels Angabe des Datums der Umsetzung melden. Der Anbieter verpflichtet sich, alle Abhilfemaßnahmen binnen neunzig (90) Tagen, nachdem dieser die Bewertung oder den Prüfbericht erhalten hat, umzusetzen oder innerhalb einer alternativen Frist, unter der Voraussetzung, dass diese Frist im gegenseitigen

Einvernehmen schriftlich nicht später als dreißig (30) Tage nach Erhalt der Bewertung oder des Prüfberichts durch den Anbieter vereinbart wird.

21.6 Der Anbieter verpflichtet sich, sich gegenwärtig und auch weiterhin an alle anwendbaren, von der Regierung angeordneten Sicherheitsstandards und Berichtspflichten sowie an die ISO 27001/27002 zu halten. Sofern der Anbieter Umgang mit Nummern von Zahlungskonten oder sonstigen damit verbundenen Zahlungsinformationen hat, bestätigt der Anbieter seine aktuelle als auch weitere Einhaltung der aktuellsten Version des Payment Card Industry Data Security Standard (PCI-DSS), und zwar in Bezug auf alle Systeme in ihrem vollen Umfang, die mit diesen Informationen Kontakt haben. Für den Fall, dass sich der Anbieter für einen Teil der umfassenden Systeme, über die PCI-gültige Daten abgewickelt werden, nicht an den PCI-DSS hält, wird dieser CWT umgehend darüber informieren und unverzüglich Anstrengungen in die Wege leiten, um diese Nichteinhaltung zu beheben sowie auf Anfrage CWT in regelmäßigen Abständen über den Stand einer solchen Korrektur informieren.

22. Standards, Best Practices, Vorschriften und Gesetze

Für den Fall, dass der Anbieter personenbezogene Daten von CWT und geschützte Unternehmensdaten verarbeitet, auf diese zugreift, diese anschaut, speichert oder verwaltet, die sich auf Mitarbeiter, Partner oder verbundene Unternehmen von CWT; Kunden von CWT; oder auf Mitarbeiter, Auftragnehmer oder Unterauftragnehmer von CWTs Kunden beziehen, verpflichtet sich der Anbieter, technische und organisatorische Sicherheitsmaßnahmen einzusetzen, die nicht weniger streng als jene sind, wie sie von Richtlinien, Vorschriften, Leitlinien und Gesetzen auf globaler, regionaler, Bundes-, Landes- oder lokaler Ebene vorgegeben werden.

23. Änderung

CWT behält sich das Recht vor, die vorliegenden Informationssicherheitsanforderungen bei Bedarf zu ändern, indem es die aktuellste Fassung auf seiner Website veröffentlicht.

Die nachstehenden Bestimmungen gelten, sofern sie nicht bereits im Hauptvertrag enthalten sind. Sollte es zwischen den folgenden Bestimmungen und denen des Vertrags zu Widersprüchen kommen, sind die Bestimmungen des Vertrags maßgebend.

24. Gewährleistungen und Pflichten

Der Anbieter gewährleistet und sichert zu, dass er während der Vertragslaufzeit und danach (soweit zutreffend mit Bezug auf die Pflichten des Anbieters gemäß Klausel zum Fortbestehen der Pflichten im Vertrag) gegenwärtig zum Zeitpunkt des Vertrags pflichtkonform ist und sich auch weiterhin an die in diesem Dokument festgehaltenen Pflichten im weiteren Verlauf des Dienst-, Software- oder Produktangebots halten wird. Mit den Bestimmungen der vorliegenden Informationssicherheitsanforderungen werden keine strengeren Sicherheits- oder sonstigen Verpflichtungen des Vertrags begrenzt.

25. Fortbestehen

Rechte und Pflichten gemäß den vorliegenden Informationssicherheitsanforderungen, einschließlich der Geheimhaltung der vertraulichen Informationen von CWT, bestehen auch nach der aktiven Laufzeit oder nach Beendigung des Vertrags fort. Alle anderen Pflichten enden ab dem Zeitpunkt, ab dem sich der Anbieter vertrauliche Informationen von CWT nicht mehr ansieht, auf diese zugreift, diese sammelt, pflegt, verarbeitet oder speichert; Räumlichkeiten von CWT nicht länger aufsucht oder vertrauliche Informationen von CWT nicht mehr aufbewahrt.

26. Laufzeit und Beendigung

26.1 Verstöße gegen Bestimmungen der vorliegenden Informationssicherheitsanforderungen stellen einen wesentlichen Verstoß im Hinblick auf den Zweck des Vertrags dar und begründen CWTs Recht auf Widerruf, Änderung oder Rechtsbehelf; die Wahl obliegt dabei CWT. Sollte es zu einem Verstoß durch den Anbieter kommen und sollte sich CWT in diesem Zusammenhang dazu entscheiden, den Vertrag nicht durchzusetzen oder nicht zu beenden, stellt diese Entscheidung keine Änderung des Vertrags dar und auch keinen Verzicht auf CWTs Rechte gemäß dem Vertrag.

26.2 Der Anbieter stimmt zu, dass ein Zugriff auf vertrauliche Informationsressourcen, welcher gegen die vorliegenden Informationssicherheitsanforderungen, CWTs Anweisungen oder Branchenstandards verstößt, sowie Datenpannen oder Störfalle, CWT einen unmittelbaren und irreparablen Schaden zufügen können, für den ein Schadenersatz in Geldform unter Umständen keinen ausreichenden Rechtsbehelf darstellt. Vor diesem Hintergrund stimmt der Anbieter zu, dass CWT hinsichtlich Verstößen oder Störfällen dieser Art neben den Rechtsmitteln, die dem Unternehmen dem Gesetz nach zustehen, ohne Nachweis der tatsächlichen Schäden die effektive Vertragserfüllung, einen Unterlassungsanspruch oder ein sonstiges billigkeitsrechtliches Rechtsmittel erwirken kann.

Version 2.0
Datum: 15. Dezember 2017