

Anlage zur Auftragsverarbeitung – DSGVO

Diese Anlage zur Auftragsverarbeitung („AV“ oder „Anlage“) ist Bestandteil der bestehenden Vereinbarung(en) zwischen dem Kunden und CA und/oder sonstigen elektronischen Vereinbarungen zwischen CA und dem Kunden hinsichtlich des Erwerbs der von CA angebotenen Services (die „Vereinbarung“) und umfasst die Vereinbarung zwischen den Parteien hinsichtlich der Verarbeitung von personenbezogenen Kundendaten gemäß den Anforderungen der Datenschutzgesetze. Das Datum des Inkrafttretens dieser AV ist das Datum der letzten Unterschrift einer Partei unten. Alle groß geschriebenen Begriffe, die hierin nicht definiert sind, haben die in der Vereinbarung genannte Bedeutung.

1. ALLGEMEINE BESTIMMUNGEN

Diese AV gilt für die Verarbeitung von personenbezogenen Daten im Rahmen der EU-Datenschutz-Grundverordnung 2016/679 (nachfolgend in Abschnitt 11 näher definiert und nachfolgend „DSGVO“) durch CA im Namen des Kunden. Seit dem 25. Mai 2018 verarbeitet CA personenbezogene Daten gemäß den Anforderungen der DSGVO, die direkt für die Bereitstellung der Services von CA gelten. Diese AV schränkt die zuvor in Kundenvereinbarungen ausgehandelten Datenschutzbestimmungen hinsichtlich der Verarbeitung von Kundendaten (einschließlich bereits bestehender Anlagen zur Auftragsverarbeitung zu der Vereinbarung) nicht ein.

Durch Unterzeichnen dieser Anlage willigt der Kunde in seinem eigenen Namen sowie im Namen und Auftrag seiner autorisierten verbundenen Unternehmen (sofern nach geltenden Datenschutzgesetzen erforderlich) in die AV ein, wenn und soweit CA personenbezogene Daten verarbeitet, bei denen diese autorisierten verbundenen Unternehmen als Verantwortliche auftreten. Ausschließlich für die Zwecke dieser AV beinhaltet der Begriff „Kunde“ sowohl den Kunden als auch autorisierte verbundene Unternehmen, sofern nichts anderes angegeben ist.

Im Rahmen der Bereitstellung der Services für den Kunden gemäß der Vereinbarung kann CA personenbezogene Daten im Namen des Kunden verarbeiten. CA willigt ein, die folgenden Bestimmungen in Bezug auf die für den Kunden in Verbindung mit der Bereitstellung der Services verarbeiteten personenbezogenen Daten zu befolgen. Sofern im jeweiligen Abschnitt nicht anderweitig definiert, sind alle Definitionen für diese AV in Abschnitt 11, „Definitionen“, zusammengefasst.

2. VERARBEITUNG VON PERSONENBEZOGENEN DATEN

2.1 Die Parteien kommen überein, dass hinsichtlich der Verarbeitung von personenbezogenen Daten der Kunde der Verantwortliche und CA der Auftragsverarbeiter ist. CA oder Mitglieder der CA Group setzen gemäß den Anforderungen in Abschnitt 5, „Unterauftragsverarbeiter“, Unterauftragsverarbeiter ein.

2.2 Der Kunde wird personenbezogene Daten bei Empfang und Verwendung gemäß den Anforderungen der Datenschutzgesetze verarbeiten und sicherstellen, dass seine Anweisungen zur Verarbeitung von personenbezogenen Daten den Datenschutzgesetzen entsprechen. Der Kunde ist allein verantwortlich für die Genauigkeit, Qualität und Rechtmäßigkeit von personenbezogenen Daten und der Art, wie er diese erwirbt.

2.3 CA verarbeitet personenbezogene Daten gemäß den geltenden Datenschutzgesetzen und den Anforderungen der DSGVO, die direkt für die Bereitstellung der Services von CA gelten. CA verarbeitet personenbezogene Daten nur im Namen des Kunden gemäß dessen dokumentierten Anweisungen und behandelt personenbezogene Daten als vertrauliche Informationen. Der Kunde weist CA an, personenbezogene Daten für die folgenden Zwecke zu verarbeiten: (i) Verarbeitung gemäß der Vereinbarung und geltenden Anweisungen, (ii) Verarbeitung zur angemessenen Befolgung der Anweisungen des Kunden (z. B. per Support-Ticket), sofern diese Anweisungen den Bedingungen der Vereinbarung entsprechen, und (iii) Verarbeitung von personenbezogenen Daten, sofern dies nach

den für CA oder CA-Verbundunternehmen geltenden Gesetzen erforderlich ist, einschließlich, aber nicht ausschließlich den geltenden Datenschutzgesetzen, in welchem Falle CA oder das betroffene CA-Verbundunternehmen den Kunden über diese gesetzlich vorgeschriebene Verarbeitung von personenbezogenen Daten informiert, sofern dies durch geltende Gesetze zulässig ist.

2.4. Gemäß Artikel 28(3) der DSGVO sind der Gegenstand und die Dauer, die Art und der Zweck der Verarbeitung sowie die Arten von personenbezogenen Daten und Kategorien von betroffenen Personen in Anhang I zu dieser Anlage zur Auftragsverarbeitung festgehalten („Anhang 1: Details zur Verarbeitung von personenbezogenen Kundendaten“). Der Gegenstand der Verarbeitung von personenbezogenen Daten durch CA ist die Erbringung der Services gemäß der Vereinbarung. Nach vorheriger schriftlicher Ankündigung kann der Kunde angemessene Korrekturen an Anhang 1 verlangen, die der Kunde als notwendig erachtet, um die Anforderungen von Artikel 28(3) der DSGVO zu erfüllen, und CA wird diese angeforderten Änderungen entsprechend prüfen. Keine der Bestimmungen in Anhang 1 übertragen einer der Parteien in dieser Anlage irgendwelche Rechte oder Pflichten.

3. RECHTE BETROFFENER PERSONEN

3.1. CA wird den Kunden, sofern gesetzlich zulässig, umgehend informieren, wenn CA von einer betroffenen Person kontaktiert wird, die von ihrem Recht auf Auskunft, Recht auf Berichtigung, Recht auf Einschränkung der Verarbeitung, Recht auf Löschung („Recht auf Vergessenwerden“), Recht auf Datenübertragbarkeit, Widerspruchsrecht zur Verarbeitung oder Widerspruchsrecht gegen automatische Entscheidungen („**Anforderung der betroffenen Person**“) Gebrauch machen möchte. Abhängig von der Art der Verarbeitung wird CA den Kunden durch angemessene technische und organisatorische Mittel bestmöglich dabei unterstützen, die Pflichten des Kunden hinsichtlich der Beantwortung einer Anforderung einer betroffenen Person gemäß Kapitel III der DSGVO zu erfüllen. CA wird, sofern dies nicht gesetzlich erforderlich ist, auf solche Anforderungen von betroffenen Personen nicht reagieren, ohne zuvor die schriftliche Einwilligung des Kunden einzuholen, ausgenommen einer Bestätigung, dass sich die Anforderung auf den Kunden bezieht.

3.2 Darüber hinaus wird CA, sofern der Kunde im Rahmen der Nutzung der Services nicht in der Lage ist, eine Anforderung einer betroffenen Person zu bearbeiten, auf Bitte des Kunden diesem in einem wirtschaftlich vertretbaren Rahmen dabei helfen, auf eine solche Anforderung einer betroffenen Person zu reagieren, vorausgesetzt, CA ist dazu gesetzlich berechtigt und die Anforderung der betroffenen Person unterliegt den geltenden Datenschutzgesetzen. Alle aus einer solchen Hilfeleistung entstehenden Kosten sind, sofern gesetzlich zulässig, vom Kunden zu tragen.

4. PERSONAL

4.1 CA wird sicherstellen, dass sein mit der Verarbeitung von personenbezogenen Daten betrautes Personal Kenntnis hat über die Vertraulichkeit der personenbezogenen Daten und entsprechend seiner Verantwortung geschult wird. Darüber hinaus gelten für dieses Personal Vertraulichkeitsauflagen, die auch über deren Beschäftigungsverhältnis bei CA hinaus Bestand haben.

4.2 CA wird wirtschaftlich vertretbare Maßnahmen ergreifen, um die Zuverlässigkeit des Personals von CA sicherzustellen, das für die Verarbeitung von personenbezogenen Daten zuständig ist.

4.3 CA muss sicherstellen, dass innerhalb der CA Group nur diejenigen Mitarbeiter auf personenbezogene Daten zugreifen können, die diese zur Erbringung der Vertragsleistung benötigen.

4.4 Datenschutzbeauftragter. Mitglieder der CA Group haben einen Datenschutzbeauftragten ernannt, sofern dies durch Datenschutzgesetze erforderlich ist. Die ernannte Person kann über datatransfers@ca.com erreicht werden.

5. UNTERAUFTRAGSVERARBEITER

5.1 Der Kunde erkennt an und willigt ein, dass (a) die verbundenen Unternehmen von CA als Unterauftragsverarbeiter eingesetzt werden können und (b) CA und dessen verbundene Unternehmen externe Unterauftragsverarbeiter in Verbindung mit der Bereitstellung der Services beauftragen dürfen. Solche Unterauftragsverarbeiter erhalten personenbezogene Daten ausschließlich zum Zweck der Bereitstellung der Services, für die sie von CA beauftragt wurden, und dürfen die personenbezogenen Daten nicht für andere Zwecke verwenden.

5.2 CA haftet für die Handlungen und Versäumnisse seiner Unterauftragsverarbeiter im selben Maße, als wenn CA die an die Unterauftragsverarbeiter ausgelagerten Services direkt gemäß den Bedingungen dieser AV bereitstellen würde, sofern dies in der Vereinbarung nicht anders festgelegt ist.

5.3 CA oder dessen verbundene Unternehmen haben mit allen Unterauftragsverarbeitern schriftliche Vereinbarungen getroffen, die auch die Verpflichtungen hinsichtlich Datenschutz umfassen und bezüglich des Schutzes von personenbezogenen Daten keinen geringeren Umfang haben als durch diese Anlage festgelegt und die die Anforderungen von Artikel 28(3) der DSGVO oder entsprechender Bestimmungen anderer Datenschutzgesetze erfüllen, sofern dies für die Art der vom Unterauftragsverarbeiter bereitgestellten Services anwendbar ist.

5.4 Der Kunde ermächtigt CA und seine verbundenen Unternehmen, Unterauftragsverarbeiter gemäß diesem Abschnitt 5 zu beauftragen. Die Liste der von CA in Verbindung mit der Bereitstellung der Services eingesetzten Unterauftragsverarbeiter ist in Anhang 2 enthalten und umfasst alle Identitäten und Geschäftssitze der Unterauftragsverarbeiter („**Liste der Unterauftragsverarbeiter**“). Falls CA die Liste ändert oder weitere Unterauftragsverarbeiter hinzufügt, ist die aktuelle Liste der Unterauftragsverarbeiter für den Kunden einsehbar unter: <https://support.ca.com/us/product-content/admin-content/subprocessor-list.html>, sodass der Kunde die Möglichkeit hat, solchen Änderungen zu widersprechen (siehe Abschnitt 5.5 unten).

5.5. Der Kunde kann der Verwendung von neuen Unterauftragsverarbeitern durch CA widersprechen. Hierfür ist eine schriftliche Mitteilung an CA innerhalb von zehn (10) Geschäftstagen nach der Aktualisierung der Liste der Unterauftragsverarbeiter durch CA erforderlich. Im Fall eines solchen Widerspruchs wird CA wirtschaftlich vertretbare Maßnahmen ergreifen, um den Widerspruch des Kunden zu behandeln, und dem Kunden diese ergriffenen Maßnahmen angemessen erläutern.

5.6. Datenübermittlungen. CA darf personenbezogene Daten des Kunden nur im gesetzlichen Rahmen im Einklang mit geltenden Datenschutzgesetzen übermitteln. Die personenbezogenen Daten werden gemäß den unter <https://www.ca.com/us/legal/privacy/data-transfers.html> dargelegten Angaben und Bestimmungen von CA übermittelt. Ausschließlich für die Bereitstellung der Services für den Kunden gemäß der Vereinbarung und den Bestimmungen aus Abschnitt 5.6 autorisiert der Kunde CA hiermit, personenbezogene Daten routinemäßig an lokale CA-Rechtsträger und/oder genehmigte Unterauftragsverarbeiter von CA zu übermitteln. Ungeachtet dessen befolgt CA im Fall, dass personenbezogene Daten des Kunden aus der Europäischen Union, dem Europäischen Wirtschaftsraum und/oder deren Mitgliedsstaaten, der Schweiz und dem Vereinigten Königreich an Länder übermittelt werden, die kein angemessenes Datenschutzniveau im Sinne der Datenschutzgesetze der vorgenannten Gebiete sicherstellen („**Eingeschränkte Übermittlungen**“), die Bestimmungen von Abschnitt 5.6(a) hinsichtlich solcher eingeschränkter Übermittlungen.

(a) **Übermittlungsarten für eingeschränkte Datenübermittlungen.** CA stellt die unten genannten Übermittlungsarten bereit, die hinsichtlich aller eingeschränkten Übermittlungen im Sinne dieser AV gelten, sofern solche Übermittlungen den folgenden Datenschutzgesetzen unterliegen:

- (1) **Selbstzertifizierung gemäß Privacy Shield.** CA hat seine Einhaltung des EU-US Privacy Shield-Programms zertifiziert. Diese Zertifizierung gilt solange, wie CA personenbezogene Daten im EWR verarbeitet. Sollten EU-Behörden oder EU-Gerichte zu dem Schluss kommen, dass Privacy Shield keine angemessene Basis für Datenübermittlungen ist, müssen die Parteien umgehend zugelassene EU-Standardvertragsklauseln (Verarbeiter) unterzeichnen, die damit Bestandteil dieser Anlage werden.
- (2) **EU-Standardvertragsklauseln.** CA und seine verbundenen Unternehmen, die als Unterauftragsverarbeiter fungieren (siehe Anhang 2), haben zuvor die EU-Standardvertragsklauseln für eine Beziehung zwischen Verantwortlichem und Auftragsverarbeiter zum Nutzen des Kunden unterzeichnet.

Sofern Services von mehreren Übermittlungsarten abgedeckt sind, unterliegt die Übermittlung von personenbezogenen Daten des Kunden nur einer Übermittlungsart gemäß der folgenden Rangordnung: (i) Selbstzertifizierung gemäß Privacy Shield; (ii) EU-Standardvertragsklauseln.

6. SICHERHEIT

6.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen implementieren der Kunde und CA geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. CA ergreift geeignete technische und organisatorische Maßnahmen zur Wahrung der Sicherheit, Vertraulichkeit und Integrität von personenbezogenen Daten gemäß den Anforderungen an Auftragsverarbeiter gemäß der DSGVO, wie in Anhang 2 „Sicherheit bei der Verarbeitung – DSGVO Art. 32“ beschrieben. CA überwacht die Einhaltung dieser Sicherheitsmaßnahmen regelmäßig. CA wird die allgemeine Sicherheit der Services während der Bereitstellung dieser Services im Rahmen der anwendbaren Vereinbarung oder des zugrunde liegenden Bestellformulars nicht maßgeblich mindern.

6.2 CA wird dem Kunden auf schriftliche Anforderung in angemessenen Abständen eine Kopie der letzten für die Verarbeitung von personenbezogenen Daten des Kunden relevanten externen Audits oder Zertifizierungen von CA oder eine entsprechende Übersicht zukommen lassen, wie sie CA üblicherweise auch anderen Kunden auf Anforderung bereitstellt. CA weist dem Kunden nach angemessener schriftlicher Anforderung die Einhaltung dieser Anlage nach. Auf schriftliche Anforderungen gewährt CA dem Kunden das Recht zur Durchführung eines schriftlichen Audits durch den Kunden oder einen unabhängigen Auditor, um nachzuweisen, dass CA angemessene Verfahren in Verbindung mit der Verarbeitung von personenbezogenen Daten und zur Einhaltung dieser Anlage hat. Der Kunde wird nicht öfter als einmal jährlich von diesem Recht Gebrauch machen. Diese Informations- und Audit-Rechte gemäß diesem Abschnitt 6.2 werden in dem Maß gewährt, in dem die Vereinbarung keine Audit-Rechte gewährt, die den Anforderungen der geltenden Datenschutzgesetze entsprechen (einschließlich, sofern anwendbar, Artikel 28(3)(h) der DSGVO). Alle Informationen, die von CA und/oder im Rahmen von Audits im Sinn dieses Abschnitts bereitgestellt werden, unterliegen den Vertraulichkeitsverpflichtungen der Vereinbarung.

6.3 CA unterstützt den Kunden angemessen bei der Erfüllung seiner Verpflichtung, eine Datenschutz-Folgenabschätzung gemäß Artikel 35 und 36 der DSGVO hinsichtlich der Nutzung der Services durch den Kunden zu erstellen. CA bietet diese Unterstützung auf angemessene Anfrage des Kunden und insofern an, als der Kunde die relevanten Informationen nicht anderweitig erlangen kann und CA Zugriff auf diese Informationen hat. Darüber hinaus unterstützt CA den Kunden bei der Zusammenarbeit oder vorherigen Beratung mit Aufsichtsbehörden bei der Durchführung der Aufgaben gemäß diesem Abschnitt 6.3 im durch die DSGVO erforderlichen Rahmen.

7. UMGANG MIT UND BENACHRICHTIGUNGEN ZU SICHERHEITSVERLETZUNGEN

7.1 CA wird den Kunden umgehend und ohne schuldhaftes Verzögerung darüber informieren, wenn CA Kenntnis über eine Verletzung der Sicherheit hat, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten des Kunden führt, die von CA oder dessen Unterauftragsverarbeitern übermittelt, gespeichert oder anderweitig verarbeitet werden („**Sicherheitsverletzung**“). CA wird sich angemessen bemühen, die Ursache einer solchen Sicherheitsverletzung zu identifizieren, und wird umgehend und ohne schuldhaftes Verzögerung: (a) die Sicherheitsverletzung untersuchen, den Kunden über die Sicherheitsverletzung informieren, und dem Kunden gegebenenfalls auch diejenigen Informationen zukommen lassen, die ein Auftragsverarbeiter dem Verantwortlichen gemäß Artikel 33(3) der DSGVO mitteilen muss, sofern diese Informationen verfügbar sind, und (b) angemessene Maßnahmen ergreifen, um die Auswirkungen des Verstoßes und den daraus entstehenden Schaden möglichst gering zu halten, sofern das für CA möglich ist. Die hier genannten Verpflichtungen gelten nicht für Verstöße, die vom Kunden oder dessen autorisierten Benutzern verursacht wurden. Der Kunde wird gemäß Abschnitt 7.3 unten über den Verstoß informiert.

7.2 Die Verpflichtung von CA gemäß diesem Abschnitt, eine Sicherheitsverletzung zu melden, stellt kein Schuldeingeständnis und keine Anerkennung einer Haftbarkeit durch CA hinsichtlich der Sicherheitsverletzung dar.

7.3. CA sendet Benachrichtigungen zu Sicherheitsverletzungen nach eigenem Ermessen an eines oder mehrere der Unternehmen des Kunden, dessen technische oder administrative Kontaktpersonen per E-Mail oder über einen anderen Kommunikationskanal. Der Kunde ist selber dafür verantwortlich, sicherzustellen, dass CA jederzeit über aktuelle Kontaktdaten des Kunden verfügt.

8. RÜCKGABE UND LÖSCHUNG VON KUNDENDATEN

8.1 CA wird Kundendaten gemäß den Verfahren von CA und den Datenschutzgesetzen und/oder gemäß den Bestimmungen der Vereinbarung an den Kunden zurückgeben und/oder löschen.

8.2 Auf Anforderung des Kunden wird CA alle personenbezogenen Daten des Kunden nach Ablauf des Bereitstellungszeitraums der Services löschen oder zurückgeben und vorhandene Kopien gemäß den in Anhang 2 „Sicherheit bei der Verarbeitung – DSGVO Art. 32“ festgelegten Verfahren löschen, es sein denn, die personenbezogenen Daten müssen aufgrund geltender Datenschutzgesetze gespeichert werden.

9. ZUSÄTZLICHE BESTIMMUNGEN FÜR PERSONENBEZOGENE DATEN IN DER EU

9.1 Die Standardvertragsklauseln und zusätzlichen Bestimmungen in diesem Abschnitt 9 gelten für die Verarbeitung von personenbezogenen Daten durch CA im Rahmen der Bereitstellung der Services.

9.1.1 Die Standardvertragsklauseln gelten nur für personenbezogene Daten, die aus dem Europäischen Wirtschaftsraum (EWR) oder der Schweiz nach außerhalb des EWR oder der Schweiz entweder direkt oder per Weiterübermittlung an ein Land oder einen Empfänger übermittelt werden, das bzw. der: (i) der EU-Kommission zufolge kein angemessenes Schutzniveau für personenbezogene Daten (gemäß geltender Datenschutzgesetze) hat und (ii) nicht durch ein geeignetes Rahmenwerk abgedeckt ist, das den zuständigen Behörden oder Gerichten zufolge ein angemessenes Schutzniveau für personenbezogene Daten bietet, einschließlich, aber nicht ausschließlich verbindlicher unternehmensinterner Datenschutzvorschriften.

9.1.2 Die Standardvertragsklauseln gelten für (i) den Rechtsträger, der die Standardvertragsklauseln als Datenexporteur angewendet hat, und (ii) alle verbundenen Unternehmen (wie in der Vereinbarung definiert) des Kunden mit Sitz im Europäischen Wirtschaftsraum (EWR) und der Schweiz, die Services auf Basis einer Bestellung im Rahmen der Vereinbarung erworben haben. Im Sinne der Standardvertragsklauseln und dieses Abschnitts 9 gelten der Kunde und dessen verbundene Unternehmen als „Datenexporteure“.

9.2 Diese AV und die Vereinbarung stellen die vollständigen und endgültigen Anweisungen von Datenexporteuren an Datenimporteure zur Verarbeitung von personenbezogenen Daten dar. Alle zusätzlichen oder abweichenden Anweisungen müssen separat vereinbart werden. Für die Zwecke der Klausel 5(a) der Standardvertragsklauseln gilt Folgendes als Anweisung eines Datenexporteurs zur Verarbeitung von personenbezogenen Daten: (i) gemäß der Vereinbarung und der darin enthaltenen Anweisungen und (b) gemäß anderer angemessener Anweisungen des Kunden (z. B. per Support-Ticket), wobei diese Anweisungen im Einklang mit den Bedingungen der Vereinbarung sein müssen.

9.3 Gemäß Klausel 5(h) der Standardvertragsklauseln erkennt der Datenexporteur an und willigt ausdrücklich ein, dass die verbundenen Unternehmen von CA als Unterauftragsverarbeiter auftreten dürfen und (b) CA und dessen verbundene Unternehmen externe Unterauftragsverarbeiter in Verbindung mit der Bereitstellung der Services beauftragen dürfen. Der Datenimporteur stellt dem Kunden eine aktuelle Liste der Unterauftragsverarbeiter für die jeweiligen Services mit den Identitäten dieser Unterauftragsverarbeiter gemäß Abschnitt 5.5 dieser AV mit genaueren Informationen zur Bereitstellung der Liste der Unterauftragsverarbeiter von CA bereit.

9.4 Die Parteien kommen überein, dass in den Kopien der Vereinbarungen mit Unterauftragsverarbeitern, die gemäß Klausel 5(j) der Standardvertragsklauseln vom Datenimporteur an den Datenexporteur gesendet werden müssen, vor dem Senden alle Wirtschaftsinformationen sowie Regelungen, die mit den Standardvertragsklauseln nicht zusammenhängen, vom Datenimporteur entfernt werden können und diese Kopien vom Datenimporteur nur auf Anfrage des Datenexporteurs bereitgestellt werden.

9.5 Die Parteien kommen überein, dass die in Klausel 5(f), Klausel 11 und Klausel 12(2) der Standardvertragsklauseln genannten Audits gemäß den folgenden Spezifikationen ausgeführt werden: Auf Anfrage des Datenexporteurs und im Rahmen der aus der Vereinbarung resultierenden Vertraulichkeitspflichten wird der Datenimporteur innerhalb eines angemessenen Zeitraums nach Erhalt einer Anfrage dem Datenexporteur (oder einem unabhängigen, externen Auditor des Datenexporteurs, der kein Wettbewerber von CA ist) in dem Rahmen, in dem CA solche Informationen auch anderen Kunden zur Verfügung stellt, Informationen zur Einhaltung der in dieser AV festgehaltenen Verpflichtungen durch die CA Group in Form der durchgeführten externen Zertifizierungen und Audits bereitstellen, die in der Vereinbarung und/oder dem Dokument zu Sicherheitsmaßnahmen festgehalten sind. Der Kunde ist berechtigt, den Datenimporteur gemäß dem Abschnitt „Hinweise“ der Vereinbarung zu kontaktieren, um einen lokalen Audit der für den Schutz von personenbezogenen Daten relevanten Verfahren zu beantragen. Der Kunde erstattet dem Datenimporteur den zeitlichen Aufwand für einen solchen lokalen Audit zu den zu diesem Zeitpunkt aktuellen Tarifen für Werk- und Dienstleistungen der CA Group, die dem Datenexporteur auf Anfrage zur Verfügung gestellt werden. Vor Beginn eines solchen lokalen Audits müssen sich der Datenexporteur und Datenimporteur auf Umfang, Zeitpunkt und Dauer des Audits sowie über den Erstattungssatz, für den der Datenexporteur verantwortlich ist, einigen. Alle Erstattungssätze müssen unter Berücksichtigung der vom Datenimporteur aufgewendeten Ressourcen angemessen sein. Der Datenexporteur wird den Datenimporteur umgehend darüber informieren, wenn im Verlauf eines Audits Probleme bei der Einhaltung aufgedeckt werden.

9.6 Die Parteien kommen überein, dass der Nachweis der Löschung von personenbezogenen Daten gemäß Klausel 12(1) dem Datenexporteur vom Datenimporteur nur auf Anfrage des Datenexporteurs erbracht wird.

9.7 Im Falle von Widersprüchen oder Unklarheiten zwischen dieser AV und den Standardvertragsklauseln haben die Standardvertragsklauseln Vorrang. Wenn dieses Dokument von einer der Parteien elektronisch unterzeichnet wird, hat diese Signatur denselben rechtlichen Stellenwert wie eine handschriftliche Unterschrift.

10. PARTEIEN DIESER AV

10.1 Haftungsbeschränkung. Sämtliche, aus dieser AV und allen AVs zwischen autorisierten verbundenen Unternehmen und CA vertraglich, durch unerlaubte Handlungen oder anderweitige Gründe resultierende Haftung der einzelnen Parteien und aller ihrer verbundenen Unternehmen zusammengenommen unterliegt dem Abschnitt „Haftungsbeschränkung“ der den jeweiligen Services zugrunde liegenden Vereinbarung. Jeder Bezug auf einen solchen Abschnitt zur Haftung der Parteien bezieht sich auf die Gesamthaftung dieser Partei und aller ihrer verbundenen Unternehmen gemäß der Vereinbarung und aller AVs. Um Zweifel auszuschließen, bezieht sich jeder Verweis auf die AV in dieser AV auf diese AV einschließlich deren Anhängen, Zeitplänen und/oder Nachträgen.

10.2 Autorisierte verbundene Unternehmen und Vertragsverhältnis. Durch Ausführen dieser AV willigt der Kunde in seinem eigenen Namen sowie im Namen und Auftrag seiner autorisierten verbundenen Unternehmen (sofern nach geltenden Datenschutzgesetzen erforderlich) in diese AV ein, wenn und soweit CA personenbezogene Daten verarbeitet, bei denen diese autorisierten verbundenen Unternehmen als Verantwortliche auftreten. Jedes autorisierte verbundene Unternehmen bindet sich an die Verpflichtungen dieser AV und, sofern anwendbar, der Vereinbarung. Um Zweifel auszuschließen, sei hiermit klargestellt, dass ein autorisiertes verbundenes Unternehmen keine Vertragspartei der Vereinbarung ist oder wird, sondern nur Vertragspartei der AV ist. Zugriff auf und Verwendung der Services durch autorisierte verbundene Unternehmen muss gemäß den Bestimmungen und Bedingungen der Vereinbarung erfolgen und jedwede Verstöße gegen die Bestimmungen der Vereinbarung durch ein autorisiertes verbundenes Unternehmen gelten als Verstöße durch den Kunden. Ausschließlich für die Zwecke dieser AV beinhaltet der Begriff „Kunde“ sowohl den Kunden als auch autorisierte verbundene Unternehmen, sofern nichts anderes angegeben ist.

10.2.1 Kommunikation. Der Kunde als Vertragspartner der Vereinbarung ist weiterhin verantwortlich für die Koordinierung der Kommunikation mit CA im Rahmen dieser AV und ist berechtigt, sämtliche Kommunikation zu dieser AV im Namen seiner autorisierten verbundenen Unternehmen zu senden und zu empfangen.

10.2.2 Rechte von autorisierten verbundenen Unternehmen. Sofern ein autorisiertes verbundenes Unternehmen Vertragspartner dieser AV von CA wird, ist es im Rahmen der geltenden Datenschutzgesetze berechtigt, von den Rechten und Rechtsmitteln nach Maßgabe der folgenden Bestimmungen Gebrauch zu machen:

10.2.2.1 Sofern es durch geltende Datenschutzgesetze nicht vorgeschrieben ist, dass das autorisierte verbundene Unternehmen ein Recht oder Rechtsmittel gemäß dieser AV direkt gegen CA durchsetzt, kommen die Parteien überein, dass (i) ausschließlich der Kunde als Vertragspartner der Vereinbarung im Namen des verbundenen Unternehmens Gebrauch von diesen Rechten und Rechtsmitteln macht und (ii) der Kunde als Vertragspartner der Vereinbarung von den Rechten gemäß dieser AV nicht für jedes verbundene Unternehmen separat, sondern für alle autorisierten verbundenen Unternehmen gemeinsam Gebrauch macht.

11. DEFINITIONEN

„**Verbundene Unternehmen von CA**“ bezeichnet jede Gesellschaft, die von CA kontrolliert wird, CA kontrolliert oder unter gemeinsamer Kontrolle mit CA steht.

„**CA**“ bezeichnet das CA Group Unternehmen, welches Vertragspartner dieser AV ist.

„**CA Group**“ bezeichnet CA und dessen verbundene Unternehmen, die an der Verarbeitung von personenbezogenen Daten beteiligt sind.

„**Autorisierte verbundene Unternehmen**“ bezeichnet beliebige verbundene Unternehmen des Kunden, die (a) den Datenschutzgesetzen der Europäischen Union, des Europäischen Wirtschaftsraums und/oder deren Mitgliedsstaaten, der Schweiz und/oder des Vereinigten Königreichs unterliegen und (b) die Services gemäß der Vereinbarung zwischen dem Kunden und CA nutzen darf, jedoch kein eigenes Bestellformular an CA gesendet hat und somit kein „Kunde“ im Sinne dieser Vereinbarung ist. Ausschließlich für die Zwecke dieser AV beinhaltet der Begriff „Kunde“ sowohl den Kunden als auch autorisierte verbundene Unternehmen, sofern nichts anderes angegeben ist. Um Zweifel auszuschließen, bezeichnet „**Verbundenes Unternehmen des Kunden**“ eine Gesellschaft, die im direkten oder indirekten Mehrheitsbesitz des Kunden ist oder durch eine Mehrheitsbeteiligung vom Kunden kontrolliert wird.

„**Verantwortlicher**“, „**Auftragsverarbeiter**“, „**Betroffene Person**“, „**Kommission**“, „**Mitgliedsstaat**“ und „**Aufsichtsbehörde**“ entsprechen in ihrer Definition der aus Kapitel 1, Artikel 4 der DSGVO und davon abgeleitete Begriffe sind entsprechend zu deuten.

„**Datenschutzgesetze**“ bezeichnet alle Gesetze und Bestimmungen, einschließlich Gesetze und Bestimmungen der Europäischen Union, des Europäischen Wirtschaftsraums und deren Mitgliedsstaaten, einschließlich der DSGVO (wie nachstehend definiert), die in der Vereinbarung für die Verarbeitung von personenbezogenen Daten gelten.

„**DSGVO**“ bezeichnet die EU-Datenschutz-Grundverordnung 2016/679 (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Europäischen Rats vom 27. April 2016) zum Schutz von natürlichen Personen hinsichtlich der Verarbeitung von personenbezogenen Daten und der freien Übermittlung solcher Daten und ersetzt die EU-Richtlinie 95/46/EG.

„**Personenbezogene Daten**“ bezeichnet alle Informationen zu (i) einer identifizierten oder identifizierbaren natürlichen Person und (ii) einer identifizierten oder identifizierbaren Gesellschaft (wobei solche Informationen gemäß geltender Datenschutzgesetze als personenbezogene Daten oder persönliche Daten gleichermaßen geschützt sind), wobei sowohl (i) als auch (ii) als Kundendaten (gemäß Definition in der jeweiligen Vereinbarung) sind, die in Verbindung mit der Vereinbarung bereitgestellt werden.

„**Verarbeitung**“ bezeichnet jede Aktion, die mit personenbezogenen Daten automatisch oder manuell durchgeführt wird, wie Erfassung, Aufzeichnung, Organisation, Speicherung, Anpassung oder Veränderung, Abruf, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder andere Formen der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschung oder Vernichtung („Verarbeiten“, „Verarbeitungen“ und „Verarbeitet“ haben dieselbe Bedeutung).

„**Sicherheitsverletzung**“ hat die Bedeutung gemäß Abschnitt 7 dieser Anlage.

„**Dokument zu Sicherheitsmaßnahmen**“ bezeichnet das Dokument zu Informationssicherheitsmaßnahmen (oder den anwendbaren Teil, je nachdem, welche Services der Kunde von CA erwirbt). Dieses Dokument kann jederzeit aktualisiert werden und ist auf <https://www.ca.com/content/dam/ca/us/files/supportingpieces/ca-information-security-practices.pdf> oder in der jeweiligen Vereinbarung zwischen CA und dem Kunden verfügbar.

„**Sicherheitsanhang**“ bezeichnet die technischen und organisatorischen Sicherheitsmaßnahmen, die CA zum Schutz von personenbezogenen Daten implementiert hat, wie in Anhang 2 „Sicherheit bei der Verarbeitung – DSGVO Art. 32“ festgelegt. Sofern sich Bedingungen des Dokuments für Sicherheitsmaßnahmen von CA und des Sicherheitsanhangs widersprechen, haben die Bedingungen aus Sicherheitsanhang 2 hinsichtlich der

Sicherheitsmaßnahmen und des Schutzes von personenbezogenen Daten gemäß den Anforderungen der DSGVO Vorrang.

„**Services**“ bezeichnet die Bereitstellung der Wartungs- und Support-Services und/oder Beratungs- sowie Werk- und Dienstleistungen und/oder die Bereitstellung von Software-as-a-Service (SaaS) und/oder andere Services, die gemäß der Vereinbarung bereitgestellt werden und in deren Rahmen CA personenbezogene Daten des Kunden verarbeitet.

„**Standardvertragsklauseln**“ bezeichnet die Vereinbarung gemäß der Entscheidung der EU-Kommission vom 5. Februar 2010 zu Standardvertragsklauseln für die Übermittlung von personenbezogenen Daten an Verarbeiter in Drittländern, in denen kein angemessenes Datenschutzniveau gewährleistet ist.

„**Unterauftragsverarbeiter**“ bezeichnet jeden Auftragsverarbeiter, der von CA oder einem Mitglied der CA Group beauftragt wird.

Liste der Anhänge und Anlagen

Anhang 1: Details zur Verarbeitung von personenbezogenen Kundendaten

Anhang 2: Sicherheit der Verarbeitung – Art. 32 DSGVO

Diese AV wird zwischen dem Kunden und CA ab dem Datum des Inkrafttretens abgeschlossen und wird ein bindender Bestandteil der Vereinbarung(en). Wenn dieses Dokument von einer der Parteien elektronisch unterzeichnet wird, hat diese Signatur denselben rechtlichen Stellenwert wie eine handschriftliche Unterschrift.

Eingewilligt für und im Namen von CA	Eingewilligt für und im Namen des Kunden
Rechtsträger von CA: _____	Rechtsträger des Kunden: _____
Unterschrift: _____	Unterschrift: _____
Name: _____	Name: _____
Titel: _____	Titel: _____
Datum: _____	Datum: _____

ANHANG 1: DETAILS ZUR VERARBEITUNG VON PERSONENBEZOGENEN DATEN

Dieser Anhang 1 enthält bestimmte Details zur Verarbeitung von personenbezogenen Kundendaten gemäß Artikel 28(3) DSGVO (oder sofern anwendbar gleichwertige Bestimmungen eines anderen Datenschutzgesetzes).

Gegenstand und Dauer der Verarbeitung von personenbezogenen Kundendaten

Gegenstand und Dauer der Verarbeitung von personenbezogenen Kundendaten sind in der Hauptvereinbarung und dieser Anlage festgelegt.

Art und Zweck der Verarbeitung von personenbezogenen Kundendaten

Art:

- Erfassung
- Aufzeichnung
- Offenlegung
- Löschung
- Änderung
- Einschränkung
- Nutzung

Zweck:

Personenbezogene Kundendaten werden genutzt, um gemäß der Hauptvereinbarung Support oder Software-as-a-Service (SaaS) bereitzustellen.

Arten von zu verarbeitenden personenbezogenen Kundendaten

- | | |
|--------------------------------------|-------------------------------------|
| Kundendaten von natürlichen Personen | <input checked="" type="checkbox"/> |
| Kundendaten von Unternehmen | <input checked="" type="checkbox"/> |
| Mitarbeiterdaten | <input checked="" type="checkbox"/> |
| Sonstige personenbezogene Daten | <input type="checkbox"/> |

Die Kategorien von betroffenen Personen, auf die sich die personenbezogenen Kundendaten beziehen

Besondere Kategorien von personenbezogenen Daten (Art. 9 DSGVO)

- | | |
|---|--------------------------|
| Gesundheitsdaten oder Daten zum Sexualleben | <input type="checkbox"/> |
| Gewerkschaftszugehörigkeit | <input type="checkbox"/> |
| Religiöse oder weltanschauliche Überzeugungen | <input type="checkbox"/> |
| Politische Meinungen | <input type="checkbox"/> |
| Rassische und ethnische Herkunft | <input type="checkbox"/> |

Die Rechte und Pflichten des Kunden und seiner verbundenen Unternehmen

Die Rechte und Pflichten des Kunden und seiner verbundenen Unternehmen sind in der Vereinbarung und der AV, einschließlich aller Anhänge, Anlagen oder Zeitpläne zur AV festgelegt.

ANHANG 2 – SICHERHEIT DER VERARBEITUNG – ART. 32 DSGVO

Vorbemerkung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen implementieren der Verantwortliche und der Auftragsverarbeiter angemessene technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, darunter u. a., sofern angemessen:

§ 1 Technische und organisatorische Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus (Software-as-a-Service und On-Premise)

(1a) Maßnahmen zur Pseudonymisierung/Anonymisierung von personenbezogenen Daten:

In diesem Produkt gespeicherte Daten sind in der Regel nicht von der Art, dass eine Pseudonymisierung oder Anonymisierung erforderlich wäre. Gegebenenfalls muss sich der Kunde an CA wenden.

On-Premise:

Nicht zutreffend

(1b) Maßnahmen zur Verschlüsselung von personenbezogenen Daten:
--

VERSCHLÜSSELUNG

Alle Daten werden während der Übermittlung mit TLS (1.0 bis 1.2 unterstützt, 1.0 und 1.1 demnächst eingestellt) verschlüsselt. Darüber hinaus werden Kundendaten auf allen Servern und Geräten verschlüsselt, die das Gelände von CA zu Backup oder Speicherung an einem anderen Standort (sofern anwendbar) verlassen. Mithilfe einer Passwortverwaltung werden die Vertraulichkeit, Integrität und Verfügbarkeit der kryptografischen Schlüssel gewährleistet. Die Nutzung von Verschlüsselungsprodukten entspricht lokalen Einschränkungen und Bestimmungen zur Verwendung von Verschlüsselung in der jeweils gültigen Rechtsprechung.

Verschlüsselungsrichtlinie

Es liegt eine Datensicherheitsrichtlinie für den Umgang mit Verschlüsselungen vor. Die Verschlüsselungsstärke für Kundendaten während der Übermittlung ist darin festgelegt.
--

Passwortverwaltung für Verschlüsselungen
--

Die Verfahren zur Passwortverwaltung für Verschlüsselungen sind dokumentiert und automatisiert. Es werden Produkte oder Lösungen bereitgestellt, um die Verschlüsselung der Datenverschlüsselungsschlüssel zu gewährleisten (z. B. softwarebasierte Lösung, Hardware Security Modules (HSM)).

Einsatz von Verschlüsselung

Bei der Übermittlung von Kundendaten über das öffentliche Internet werden diese immer über einen verschlüsselten Kanal übertragen. Die Details zur Verschlüsselung werden dokumentiert, wenn die Übermittlung automatisiert erfolgt. Freigegebenes, dediziertes Personal ist für die Verschlüsselung und Entschlüsselung der Daten verantwortlich, sofern diese manuell erfolgt. Kundendaten müssen auch bei der Übermittlung über beliebige Netzwerke verschlüsselt werden. VPN-Übertragungen erfolgen über einen verschlüsselten Kanal.

On-Premise:

Der Verantwortliche stellt dem Auftragsverarbeiter Daten für Support-Fälle verschlüsselt bereit. Jeder Fall wird in einer sicheren Umgebung gelöst. 30 Tage nach Abschluss eines Falls werden die Daten zu dem Support-Fall gelöscht.

(1c) Maßnahmen zur Sicherstellung der **fortwährenden Vertraulichkeit** von personenbezogenen Daten:

Sämtlicher Zugang zu den Rechenzentren, in denen Kundendaten gespeichert werden, ist gemäß der Informationszugangskontrollrichtlinie von CA und der Aufgabentrennungsrichtlinie von CA auf das Betriebsteam von CA beschränkt. CA befolgt dabei den Grundsatz der Rechtebeschränkung und gewährt Zugang nur basierend auf Rolle und geschäftlichem Anwendungsfall. Zugangsrechte werden regelmäßig sowie bei einer Änderung der Rolle oder dem Ausscheiden eines Mitarbeiters geprüft. Der Zugang zu einer Umgebung, in der Kundendaten gespeichert werden, wird streng kontrolliert und überwacht. Der Kunde ist für die Verwaltung des Zugriffs auf seine Abonnementdaten sowie den Lebenszyklus dieser Konten verantwortlich. Die Administratoren der Kundenabonnements sind für die Benutzerverwaltung und zugehörigen Passwortrichtlinien innerhalb der Anwendung verantwortlich. Der Kunde ist für den Lebenszyklus dieses Kontos verantwortlich.

On-Premise:

Die Arbeit erfolgt in einer sicheren Umgebung, Datenübermittlungen sind gesichert. Daten werden nach Abschluss eines Support-Falls gelöscht.

(1d) Maßnahmen zur Sicherstellung der **fortwährenden Integrität** von personenbezogenen Daten:

DATENINTEGRITÄT

Die Richtlinien und Verfahren von CA Technologies sollen sicherstellen, dass alle gespeicherten, empfangenen, verwalteten oder anderweitig zugreifbaren Daten nicht kompromittiert werden und intakt bleiben. Es sind Verfahren zur Validierung der Datenintegrität implementiert.

Datenübermittlungskontrollen

Die Prozesse und Verfahren der Datenübermittlungskontrolle zur Sicherstellung der Datenintegrität sind dokumentiert. Die Datenintegrität wird nach der Übertragung mithilfe von Prüfsummen und Anzahlen validiert.

Datentransaktionskontrolle

Die Kontrollen zur Verhinderung und Identifizierung von doppelten Transaktionen in Finanzmitteilungen werden dokumentiert. Digitale Zertifikate (z. B. digitale Signaturen, Server-zu-Server) zur Sicherstellung der Datenintegrität während der Übermittlung folgen einem dokumentierten Prozess und Verfahren.

On-Premise:

Nicht anwendbar; Daten werden nach Abschluss eines Support-Falls gelöscht, siehe Abschnitt 2 a) bis e).

(1e) Maßnahmen zur Sicherstellung der **fortwährenden Verfügbarkeit von Verarbeitungssystemen und -services:**

VERFÜGBARKEITSKONTROLLE

- Schutz vor Feuer und Maßnahmen im Fall von Stromausfällen in den Rechenzentren einschließlich Backup

Physische Kontrollen

CA Technologies hat effektive Kontrollmechanismen implementiert, um Daten vor physischem Zugriff durch böswillige oder unautorisierte Personen zu schützen. Die physischen Kontrollen für die gesamte Anlage sind dokumentiert. Für Server-/Computer-/Telekommunikationsräume werden gegenüber allgemeinen Bereichen weitere Zugangsbeschränkungen umgesetzt.

Backup und Lagerung an einem anderen Standort

CA Technologies hat eine festgelegte Backup-Richtlinie und entsprechende Verfahren für regelmäßige und planmäßige Datenbackups implementiert. Für den Schutz von gesicherten Daten (lokal und an einem anderen Standort) sind effektive Kontrollen implementiert. CA Technologies stellt außerdem sicher, dass die Übermittlung bzw. der Transport von Kundendaten von und zu den Backup-Orten auf sichere Weise erfolgt. Darüber hinaus führt CA Technologies regelmäßig Tests durch, um sicherzustellen, dass Daten von Backup-Geräten sicher wiederhergestellt werden können.

Backup-Prozess

Die Verfahren für Backups und Lagerung an einem anderen Standort sind dokumentiert. Die Verfahren umfassen auch eine vollständige Wiederherstellung von Anwendungen und Betriebssystemen. Die erfolgreiche Wiederherstellung von Backup-Medien wird regelmäßig getestet. Umgebungskontrollen (z. B. Feuchtigkeit, Temperatur) sind lokal in den Bereitstellungsbereichen dokumentiert und präsentiert.

Vernichtung von Backup-Medien

Für die Schulung von Personal zu den angemessenen Methoden zur Vernichtung von Backup-Medien sind entsprechende Verfahren definiert. Die Vernichtung von Backup-Medien durch Dritte wird (beispielsweise durch einen Vernichtungsnachweis) durch festgelegte Verfahren dokumentiert.

Lagerung an einem anderen Standort

Ein Plan für physische Sicherheit für die externe Anlage ist dokumentiert. Obligatorische Zugangskontrollen finden an Eingängen und Zugängen zu Lagerräumen statt. Der Zugang zu der externen Anlage ist eingeschränkt und wird nur nach einem Freigabeprozess gewährt. Die elektronische Übermittlung von Daten an einen anderen Standort erfolgt über einen verschlüsselten Kanal.

On-Premise:

Abgeschlossene Umgebung, nicht anwendbar. Die Daten verbleiben beim bestehenden Verantwortlichen.

(1f) Maßnahmen zur Sicherstellung der **fortwährenden Belastbarkeit von Verarbeitungssystemen und -services:**

ÜBERWACHUNG VON SCHWACHSTELLEN

CA Technologies erfasst und analysiert fortwährend Informationen zu neuen und vorhandenen Bedrohungen und Schwachstellen, tatsächlichen Angriffen auf die Einrichtung oder andere sowie die Effektivität der bestehenden Sicherheitsmaßnahmen. Überwacht werden folgende Bereiche: Richtlinien und Verfahren, Viren und bösartiger Code, Eindringungserkennung sowie Ereignis- und Zustandsüberwachung. Mithilfe von Protokollen lassen sich Sicherheitsvorfälle effektiv hervorheben und untersuchen.

Richtlinie und Verfahren zu Schwachstellen

Es werden Eindringungs-/Schwachstellentests an den internen/externen Netzwerken und/oder spezifischen Hosts durchgeführt. Die Tests werden in der Regel extern von namhaften externen Unternehmen durchgeführt. Die Kundenumgebungen sind im Rahmen dieser Tests mit abgedeckt. Alle Problembereiche mit hohem Risiko werden innerhalb eines angemessenen Zeitrahmens behoben.

Antivirus und bösartiger Code

Die Server, Workstations und Internet-Gateway-Geräte werden regelmäßig mit aktuellen Antivirendefinitionen aktualisiert. Alle Antiviren-Aktualisierungen werden durch festgelegte Verfahren hervorgehoben. Die Antiviren-Tools sind für wöchentliche Scans, Virenerkennung, Dateischreibvorgänge in Echtzeit und Aktualisierungen von Signaturdateien konfiguriert. Laptops und Remote User sind ebenfalls durch Antiviren-Tools geschützt. Verfahren zum Erkennen und Beseitigen von nicht autorisierten und nicht unterstützten Anwendungen (z. B. Freeware) sind dokumentiert.

Warnungen enthalten die folgenden Attribute:

- Eindeutige Kennung
- Datum
- Zeit
- Prioritätsniveau-ID
- Quell-IP-Adresse
- Ziel-IP-Adresse
- Ereignisbeschreibung
- Benachrichtigung an Sicherheitsteam gesendet
- Ereignisstatus

Überwachung auf Sicherheitsereignisse

Sicherheitsereignisse werden protokolliert (Protokolldateien), überwacht (durch dedizierte Personen) und behandelt (zeitnahe Aktionen werden dokumentiert und ausgeführt). Netzwerkkomponenten, Workstations, Anwendungen sowie alle Überwachungs-Tools sind für die Überwachung von Benutzeraktivitäten konfiguriert. Es sind organisatorische Verantwortungen für die Reaktion auf Ereignisse definiert. Es werden Prüftools (oder andere Protokolle) eingesetzt, um wichtige Änderungen an der Systemkonfiguration aufzuzeichnen. Die Protokollberechtigungen schränken die Änderung durch Administratoren ein. Der Aufbewahrungszeitraum für die verschiedenen Protokolle ist definiert und wird befolgt.

(1g) Maßnahmen zur Wiederherstellung der **Verfügbarkeit von und des Zugangs zu personenbezogenen Daten im Fall eines technischen oder physischen Vorfalls:**

Siehe oben unter VERFÜGBARKEITSKONTROLLE

VORFALLSREAKTION

CA Technologies dokumentiert einen Plan sowie die zugehörigen Verfahren im Fall eines Informationssicherheitsvorfalls. Im Vorfallsreaktionsplan sind die Pflichten der Mitarbeiter klar umrissen und relevante zu benachrichtigende Parteien benannt. Das Vorfallsreaktionsteam wird entsprechend geschult. Die Durchführung des Vorfallsreaktionsplans wird regelmäßig getestet.

Vorfallsreaktionsprozess

Eine Richtlinie und Verfahren zur Verwaltung von Informationssicherheitsvorfällen sind dokumentiert. Die Richtlinie und/oder Verfahren zur Vorfallsverwaltung enthalten die folgenden Attribute:

- Organisationsstruktur ist definiert
- Reaktionsteam ist identifiziert
- Verfügbarkeit des Reaktionsteams ist dokumentiert
- Rechtzeitigkeit für Vorfallerkennung und Offenlegung sind dokumentiert
- Lebenszyklus für Vorfallsprozesse einschließlich der folgenden einzelnen Schritte ist definiert:
 - Identifizierung
 - Zuweisung eines Schweregrads für die einzelnen Vorfälle
 - Kommunikation
 - Lösung
 - Schulung
 - Testing (Häufigkeit prüfen)
 - Reporting
- Vorfälle müssen klassifiziert und priorisiert werden
- Im Rahmen der Vorfallsreaktion muss der Kunde über dessen Beziehungsmanager (Bereitstellung) oder eine andere im Vertrag festgelegte Kontaktperson benachrichtigt werden.

Eskalation/Benachrichtigung

Der Vorfallsreaktionsprozess wird ausgeführt, sobald CA Technologies Kenntnis über den Vorfall erlangt (unabhängig von der Tageszeit).

On-Premise:

Nur teilweise anwendbar; Daten werden nach Abschluss des Support-Falls gelöscht.

(1h) Maßnahmen für **regelmäßige Überprüfung, Bewertungen und Evaluierungen der Wirksamkeit von technischen und organisatorischen Maßnahmen:**

ORGANISATORISCHE KONTROLLE

BETRIEB

CA Technologies hat IT-Betriebsverfahren dokumentiert, um den korrekten und sicheren Betrieb seiner IT-Assets sicherzustellen.

Betriebliche Verfahren und Zuständigkeiten.

Betriebliche Verfahren sind im Betriebshandbuch dokumentiert und werden erfolgreich umgesetzt.

Das Betriebshandbuch umfasst die folgenden Bestandteile:

- Planungsanforderungen
- Fehlerbehandlung (z. B. Datentransport, Ausdrucke, Kopien)
- Erzeugen von und Umgang mit speziellen Ausgaben

Wartung und Fehlerbehebung von Systemen
Dokumentierte Verfahren zur Verwaltung der SLAs/KPIs und der Berichtsstruktur für Eskalationen

Beim Auftragsverarbeiter einschließlich des (externen) Datenschutzbeauftragten werden regelmäßig interne Sicherheits-Audits durchgeführt.

§ 2 Datenschutzbeauftragte

Name:	Kontaktdaten:
Bonnie Yeomans	CA, Inc. 520 Madison Avenue New York, NY 10022 Assistant General Counsel and Chief Privacy Officer
Yasmin Brook	CA Deutschland GmbH Marienburgstr. 35 64297 Darmstadt Deutschland Senior Counsel & Global Field Privacy Officer

§ 3 Eine aktuelle Liste der Unterauftragsverarbeiter liegt hier:
<https://support.ca.com/us/product-content/admin-content/subprocessor-list.html>

§ 4 Gesellschaften von CA, die gemäß der Hauptvereinbarung Support und Maintenance anbieten

Gesellschaften von CA		
Name	Kontaktdaten	Ort
CA Argentina S.A.	Av. Alicia Moreau de Justo 400, Piso 4, Buenos Aires, Argentina C.P. C1107AAH	Argentinien
CA (Pacific) Pty Ltd	6 Eden Park Drive, North Ryde, New South Wales 2113, Australia	Australien
CA Software Österreich GmbH	EURO PLAZA, Am Europlatz 5, Gebäude C, 1120 Vienna	Österreich
CA Belgium SA	Da Vincilaan 11, Building Figueras, B-1935 Zaventem - Belgium	Belgien
CA Programas de Computador Participacoas Servicos Ltda	Avenida Dr Chucri Zaidan, 1240 – 26º e 27º andares, Golden Tower, Vila São Francisco, CEP 04711-130 - São Paulo/SP, Brasil - CNPJ/MF 08.469.511/0001-69	Brasilien
CA Canada Company	2700 Matheson Blvd East, Suite 800E, Mississauga, Ontario, L4W 5M2, Canada	Kanada
CA de Chile, S.A.S.	Avenida Providencia, 1760, piso 15, Edificio Palladio, oficina 1501, Providencia, Chile, inscrita bajo el Registro RUT 96.724.010-9	Chile
CA CZ, s.r.o	Praha 4 - Chodov, V Parku 2316/12, PSČ 148 00	Tschechien
CA Software ApS	Borupvang 5B, DK - 2750, Ballerup, Denmark	Dänemark
CA Limited (formerly CA Plc and formerly Computer Associates Plc)	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
CA Technology R&D Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
Computer Associates Holding Ltd.	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
Computer Associates UK Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
CA SAS	Tour Opus 12, 4 Place des Pyramides, La Défense 9, 92914 Paris La Défense Cedex, France,	Frankreich
CA Computer Associates European Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Deutschland
CA Computer Associates Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Deutschland

CA Computer Associates Technology GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Deutschland
CA Deutschland GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Deutschland
CA (India) Technologies Private Limited	Ground Floor, Vibgyor Tower, Plot C-62, G-Block, Bandra Kurla Complex, Bandra (East), Mumbai - 400 051	Indien
CA Software Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israel
CA Technologies R&D Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israel
CA S.r.l.	Via Francesco Sforza 3, 20080 Milano Tre, Basiglio (MI)	Italien
CA Japan, Ltd.	JA Kyosai Bldg., 2-7-9 Hirakawa-cho, Chiyoda-ku, Tokyo 102-0093, Japan	Japan
CA Services, S.A. DE C.V.	Miguel de Cervantes Saavedra 193 piso 5, Col. Granada, 11500, Ciudad de México, México; inscrita bajo el registro CSM 9505032G1	Mexiko
CA Software de Mexico, S.A. de C.V	Siehe oben	Mexiko
CA Europe Holding B.V.	Orteliuslaan 1001, 3528 BE, Utrecht, Netherlands	Niederlande
CA software BV	Siehe oben	Niederlande
CA Software Holding BV	Siehe oben	Niederlande
CA IT Management Solutions Spain, S.L.U.	WTC Almeda Park, Edificio 2, planta 4, Plaça de la Pau s/n, 08940 Cornellá de Llobregat	Spanien

