Vereinbarung zur Auftragsverarbeitung
für Dienstleistungen der Cortado Mobile Solutions GmbH

i. S. d. Art. 28 Abs. 3 EU-Datenschutzgrundverordnung (DSGVO)

Präambel

Um die personenbezogenen Daten von Einzelpersonen besser zu schützen, stellen wir diese Vereinbarung zur Auftragsverarbeitung zur Verfügung, die unseren und Ihren Umgang mit diesen Daten regelt (im Folgenden als ***Vereinbarung*** bezeichnet). Diese Vereinbarung ergänzt die Allgemeinen Geschäftsbedingungen der Cortado Mobile Solutions GmbH (im Folgenden als ***Vertrag*** bezeichnet) – wobei diese Vereinbarung einen Anhang dazu darstellt – und keine weiteren Maßnahmen Ihrerseits erfordert.

Die Vereinbarung konkretisiert die Verpflichtungenn der Vertragsparteien zum Datenschutz. Vertragsparteien sind Sie als ***Auftraggeber*** **(Verantwortlicher)** und die **Cortado Mobile Solutions GmbH, Alt-Moabit 91a, 10559 Berlin, Deuschland** (im Folgenden als ***CMS*** bezeichnet) als ***Auftragnehmer*** **(Auftragsverarbeiter)**.
Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit den Festlegungen des Vertrages im Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (im Folgenden *Daten*) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
• Nutzer-Accounts im Active Directory des Auftraggebers • allgemeine Informationen, die bei Meetings oder Vor-Ort-Einsätzen erforderlich sind oder zufällig erfahren werden • ggf. Formulardaten auf den Webseiten des Auftrag-nehmers • ggf. Daten, die von der CMS-Software verarbeitet werden, wie Logdaten	• Kontaktdaten von Ansprechpartnern werden in der Kunden-datenbank des Auftragnehmers gespeichert und ausschließlich zum Zwecke der Erfüllung der Geschäftszwecke zwischen Auftraggeber (Verantwortlicher) und Auftragnehmer (Auftragsverarbeiter) verwendet. Insbesondere betrifft das: Name, Vorname, Position, ggf. Niederlassung des Auftraggebers, Firmen-Telefonnummer, Firmen-E Mail-Adresse • Support-, Vertriebs-, Abrechnungs- und Consulting-Leistungen	Mitarbeiter/innen, Kunden/innen oder Geschäftspartner/innen des Auftraggebers

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und auf Weisung des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutz-gesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die

Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die in der Vereinbarung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(3) Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich zu dem in § 1 beschriebenen Zweck. Diese Zweckbindung reicht der Auftragnehmer auch an alle Subauftragnehmer gemäß § 7 weiter. Ausnahme: Im Falle eines Fehlers kann es notwendig werden, Logdaten von Rechnern zur Fehleranalyse auszuwerten.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten – außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt, und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten (siehe Anlage 1).

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt – soweit vereinbart – den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Zum Zeitpunkt des Vertragsabschlusses ist dies der Datenschutzbeauftragte der Cortado Mobile Solutions GmbH:

Herr *Herbert Hemke* (dataprotection@cortado.com)

(7) Der Auftragnehmer gewährleistet, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen um seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen,.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien aufgrund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, sofern nicht im Vertrag bereits vereinbart.

(9) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Auftrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung/Vernichtung ist dem Auftraggeber auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO gilt § 3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt

den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Diese entspricht der Vergütung für Consulting-Leistungen durch den Auftragnehmer. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend – mit Ausnahme der Regelung zur Vergütung. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subauftragnehmer (weitere Auftragsverarbeiter)

(1) Der Auftraggeber stimmt zu, dass der Auftragnehmer seinerseits Subauftragnehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subauftragnehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer Frist von vier Wochen – widersprechen. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(2) Erteilt der Auftragnehmer Aufträge an Subauftragnehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung dem Subauftragnehmer zu übertragen.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subauftragnehmer durchgeführt:

Name und Anschrift des Subauftragnehmers	Beschreibung der Teilleistungen
Cortado Holding AG, Alt-Moabit 91 a/b, 10559 Berlin, Deutschland (Konzernmutter)	Geschäftstätigkeit des Konzern wie: • Administration von Webseiten, Sozialen Medien sowie Web- und Clouddiensten wie *Teamplace*, *Amazon Web Services*, *Microsoft Azure* und *Cortado MDM* • Dienstleistungen wie Marketing, Vertrieb, Kundensupport, Recruiting, Team-Management, Zahlungsabwicklung, Buchhaltung und Rechnungswesen • Vertretung des Auftragnehmers gegenüber Behörden und Unternehmen in juristischen und steuerlichen Fragen, bei Wirtschaftsprüfungen, in Fragen des Personalmanagements, der Altersvorsorge und der Gewinnbeteiligung • Sicherheitsorganisation wie IT-Administration, IT-Sicherheit, Alarmsystem und Security
Cortado Inc., 3858 Walnut St #130, Denver, CO 80205, USA (Konzerntochter)	• Dienstleistungen für den Auftragnehmer (wie Vertrieb, Consulting und Kunden-support) • nur Zugriff auf Kontaktdaten von Ansprechpartnern
Cortado Pty Ltd., Level 12, Plaza Building, Australia Square,95 Pitt Street, NSW 2000 Sydney, Australien (Konzerntochter)	• Dienstleistungen für den Auftragnehmer (wie Vertrieb, Consulting und Kunden-support) • nur Zugriff auf Kontaktdaten von Ansprechpartnern

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlichem« im Sinne der Datenschutzgrundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Mitteilung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt; dies gilt auch für den Verzicht auf dieses Formerfordernis.
Der Auftraggeber kann der Änderung bzw. Ergänzung innerhalb einer Frist von vier Wochen gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Zustimmung zur Änderung bzw. Ergänzung als gegeben.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Anlage 1: Technische und organisatorische Maßnahmen von CMS gemäß Art. 32 DSGVO

Allgemeines

- regelmäßige Datenschutz-Schulungen für alle Mitarbeiter/innen von CMS
- Datenschutz-Informationen im internen Wiki-Informationssystem von CMS
- Informationen und Maßnahmen zur Sensibilisierung der Mitarbeiter/innen von CMS gegenüber Angriffen auf die IT-Infrastruktur
- jährliche Sicherheits- und Datenschutz-Audits, bei denen u. a. Inhalt und Wirksamkeit folgender Dokumente überprüft werden:
  - Datenschutzerklärung der Cortado Mobile Solutions GmbH
  - Datenschutzerklärungen der CMS-Apps

sowie folgender Dokumente der Konzernmutter Cortado Holding AG:

- Information Security Policy
- Logical Access Control Policy + Password Policy
- Audit and Assessment Policy
- Datenschutzschulung (Data Protection Training)
- Mobile Device Policy
- Contract Policy + Non-Disclosure Policy
- Workforce Policy + Workspace and Premises Policy
- Notfallplan (Business Continuity & Incident Response Plan)
- Information Security Management Framework (ISMF)

IT-Umgebung

IT-Infrastruktur von CMS:

- Serverräume in feuertechnisch getrennten Gebäuden
- Zutrittsprotokolle für Serverräume
- Antivirensoftware auf allen PCs
- Informationssicherheitsprogramm und Intrusion-Prevention-System (IPS)
- Konzept für Reaktion auf Vorfälle
- Fernzugriff auf Server via VPN und Remotedesktop-Verbindung (RDP)
- Webplattformen auf eigenen Servern, z. B.: Confluence (Knowledge-base), Cortado Enterprise Portal (externes Self-Service-Portal für Partner und Kunden), Projektmanagement, E-Mails
- Nutzung von Cloud-Diensten, z. B. Zahlungsdienstleistungen, Online-Shops, Kundendatenbanken, Teamarbeit und Online-Speicher (Teamplace), Mobile Device Management (Cortado MDM), Microsoft Office 365, Chat-, Meeting- und Webinar-Plattformen

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungs-anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

IT-Infrastruktur von CMS:

- getrennte Serverräume für Firmendaten, Alarmanlage und Backups
- elektronisches Schließsystem mit Token und PIN
  sowie Sicherheitsschlösser mit Schlüsselregelung (manuelles Schließsystem)
- verschlossene Türen bei Abwesenheit
- Räume ohne Fenster

- Zutrittsberechtigungsregelung
- Zutrittsregelungen für Nicht-Admins und für betriebsfremde Personen
- Wachpersonal für die Zeiten, in denen die Firma nicht besetzt ist: Sicherheit Nord GmbH & Co. KG, Niederlassung Berlin, Ringstraße 44/45, 12105 Berlin, Tel. 030-70 79 20-0, www.sicherheit-nord.de
- Mitarbeiter- und Besucherausweise, Personenkontrolle am Empfang

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

IT-Infrastruktur von CMS:

- Identifizierung und Authentifizierung
- Begrenzung der Fehlversuche
- zeitgesteuerte Dunkelschaltung des Bildschirms mit Passwortschutz
- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifizierung mit Benutzername und Passwort
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz von VPN-Technologie
- Verschlüsselung der Druckdaten
- Pull-Printing (ThinPrint Personal Printing)
- Mobile Device Management: Cortado Server (z. B. zum externen Löschen von Daten, zum Sperren von Geräten und zu deren Lokalisierung)

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

IT-Infrastruktur von CMS:

- Berechtigungskonzept
- Identifizierung und Authentifizierung
- Aufbewahrung von Datenträgern in verschließbaren Schränken/Data Safes
- Monatsbackups werden in ein separates Gebäude transportiert und dort gelagert
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- pro Anwendung in der Regel spezielle Admins festgelegt
- Einsatz von Aktenvernichtern
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- sichere Aufbewahrung von Datenträgern

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist

IT-Infrastruktur von CMS:

- Transport und Lagerung von Backups (ausschließlich durch IT-Admins)
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung, wenn gewünscht, z. B. für Mailverkehr mit Wirtschaftsprüfern und Steuerberatern (Standard: S/MIME)
- Weitergabe von Daten via gesicherter Cloud-Plattform (Teamplace)
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Art. 28 Abs. 3 DSGVO).

Siehe hierzu die betreffende Datenschutzvereinbarung resp. Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO.

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

IT-Infrastruktur von CMS:

- Alarmmeldung bei unberechtigten Zutritten zu den Firmenräumen
- unterbrechungsfreie Stromversorgung (USV)
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in unmittelbarer Nähe der Serverräume
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Serverräume befinden sich nicht unter sanitären Anlagen
- Schutzsteckdosenleisten in Serverräumen
- Backup- & Recovery-Konzept
- Durchführen von Datensicherungen
- Aufbewahrung von Backups an einem sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung

Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

IT-Infrastruktur von CMS:

- physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Berechtigungskonzept
- Festlegung von Datenbankrechten
- logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- getrennte Datenbanken (pro Anwendung)

Anlage 1: Technische und organisatorische Maßnahmen von CMS gemäß Art. 32 DSGVO

Allgemeines

- regelmäßige Datenschutz-Schulungen für alle Mitarbeiter/innen von CMS
- Datenschutz-Informationen im internen Wiki-Informationssystem von CMS
- Informationen und Maßnahmen zur Sensibilisierung der Mitarbeiter/innen von CMS gegenüber Angriffen auf die IT-Infrastruktur
- jährliche Sicherheits- und Datenschutz-Audits, bei denen u. a. Inhalt und Wirksamkeit folgender Dokumente überprüft werden:
  - Datenschutzerklärung der Cortado Mobile Solutions GmbH
  - Datenschutzerklärungen der CMS-Apps

sowie folgender Dokumente der Konzernmutter Cortado Holding AG:

  - Information Security Policy
  - Logical Access Control Policy + Password Policy
  - Audit and Assessment Policy
  - Datenschutzschulung (Data Protection Training)
  - Mobile Device Policy
  - Contract Policy + Non-Disclosure Policy
  - Workforce Policy + Workspace and Premises Policy
  - Notfallplan (Business Continuity & Incident Response Plan)
  - Information Security Management Framework (ISMF)

IT-Umgebung

IT-Infrastruktur von CMS:

- Serverräume in feuertechnisch getrennten Gebäuden
- Zutrittsprotokolle für Serverräume
- Antivirensoftware auf allen PCs
- Informationssicherheitsprogramm und Intrusion-Prevention-System (IPS)
- Konzept für Reaktion auf Vorfälle
- Fernzugriff auf Server via VPN und Remotedesktop-Verbindung (RDP)
- Webplattformen auf eigenen Servern, z. B.: Confluence (Knowledge-base), Cortado Enterprise Portal (externes Self-Service-Portal für Partner und Kunden), Projektmanagement, E-Mails
- Nutzung von Cloud-Diensten, z. B. Zahlungsdienstleistungen, Online-Shops, Kundendatenbanken, Teamarbeit und Online-Speicher (Teamplace), Mobile Device Management (Cortado MDM), Microsoft Office 365, Chat-, Meeting- und Webinar-Plattformen

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungs-anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

IT-Infrastruktur von CMS:

- getrennte Serverräume für Firmendaten, Alarmanlage und Backups
- elektronisches Schließsystem mit Token und PIN
  sowie Sicherheitsschlösser mit Schlüsselregelung (manuelles Schließsystem)
- verschlossene Türen bei Abwesenheit

- Räume ohne Fenster
- Zutrittsberechtigungsregelung
- Zutrittsregelungen für Nicht-Admins und für betriebsfremde Personen
- Wachpersonal für die Zeiten, in denen die Firma nicht besetzt ist: Sicherheit Nord GmbH & Co. KG, Niederlassung Berlin, Ringstraße 44/45, 12105 Berlin, Tel. 030-70 79 20-0, www.sicherheit-nord.de
- Mitarbeiter- und Besucherausweise, Personenkontrolle am Empfang

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

IT-Infrastruktur von CMS:

- Identifizierung und Authentifizierung
- Begrenzung der Fehlversuche
- zeitgesteuerte Dunkelschaltung des Bildschirms mit Passwortschutz
- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifizierung mit Benutzername und Passwort
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz von VPN-Technologie
- Verschlüsselung der Druckdaten
- Pull-Printing (ThinPrint Personal Printing)
- Mobile Device Management: Cortado Server (z. B. zum externen Löschen von Daten, zum Sperren von Geräten und zu deren Lokalisierung)

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

IT-Infrastruktur von CMS:

- Berechtigungskonzept
- Identifizierung und Authentifizierung
- Aufbewahrung von Datenträgern in verschließbaren Schränken/Data Safes
- Monatsbackups werden in ein separates Gebäude transportiert und dort gelagert
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- pro Anwendung in der Regel spezielle Admins festgelegt
- Einsatz von Aktenvernichtern
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- sichere Aufbewahrung von Datenträgern

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist

IT-Infrastruktur von CMS:

- Transport und Lagerung von Backups (ausschließlich durch IT-Admins)
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung, wenn gewünscht, z. B. für Mailverkehr mit Wirtschaftsprüfern und Steuerberatern (Standard: S/MIME)
- Weitergabe von Daten via gesicherter Cloud-Plattform (Teamplace)
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Art. 28 Abs. 3 DSGVO).

Siehe hierzu die betreffende Datenschutzvereinbarung resp. Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO.

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

IT-Infrastruktur von CMS:

- Alarmmeldung bei unberechtigten Zutritten zu den Firmenräumen
- unterbrechungsfreie Stromversorgung (USV)
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in unmittelbarer Nähe der Serverräume
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Serverräume befinden sich nicht unter sanitären Anlagen
- Schutzsteckdosenleisten in Serverräumen
- Backup- & Recovery-Konzept
- Durchführen von Datensicherungen
- Aufbewahrung von Backups an einem sicheren, ausgelagerten Ort
- Testen von Datenwiederherstellung

Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

IT-Infrastruktur von CMS:

- physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Berechtigungskonzept
- Festlegung von Datenbankrechten
- logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- getrennte Datenbanken (pro Anwendung)