cobra® CRM

Bedingungen zur cobra PrivateCloud

§1 Gegenstand, Leistungsumfang

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig als Vertragspartner ausgewählt.

(2) Gegenstand und Dauer des Auftrags ergeben sich aus den Allgemeinen Geschäftsbedingungen des Auftragnehmers für das Produkt "cobra PrivateCloud" und aus den vorliegenden Bestimmungen zur Datenverarbeitung.

Der Auftrag umfasst insbesondere:

- Umfang, Art und Zweck der Auftragsdatenverarbeitung:
Der Auftragnehmer wird im Rahmen des vorstehenden Hauptvertrags dem Auftraggeber Speicherplatz auf einem Server im Rechenzentrum des Auftragnehmers in Deutschland bereitstellen, damit der Auftraggeber dort personenbezogene Daten erheben, verarbeiten und / oder nutzen, insbesondere speichern und / oder löschen kann. Dabei wird ausschliesslich der Auftraggeber die betreffenden personenbezogenen Daten erheben, verarbeiten und / oder nutzen. Lediglich die Speicherung und ggf. Sicherung der personenbezogenen Daten erfolgt durch den Auftragnehmer.

- Art der Daten:
Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):
- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Kreis der Betroffenen:
Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung / Beschreibung der betroffenen Personenkategorien):
- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter

(3) Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben oder mit anderen Daten zusammenzuführen. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur ordnungsgemässen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

§ 2 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist verantwortliche Stelle im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung (insbesondere die Einholung erforderlicher Einwilligungserklärungen) obliegt dem Auftraggeber. Er ist ebenfalls für die Wahrung der Betroffenenrechte verantwortlich. Der Auftraggeber erteilt sämtliche Aufträge auf zuvor mit dem Auftragnehmer abgestimmte Art und Weise.

(2) Der Auftraggeber hat das Recht, sich vor Beginn der Datenverarbeitung und sodann regelmässig, von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Massnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber ist berechtigt, das Ergebnis in geeigneter Weise zu dokumentieren. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn Fehler oder Unregelmässigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer festgestellt werden.

(4) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen. Die Weisungen können mündlich erfolgen, sollen aber zumindest nachträglich schriftlich wiederholt werden.

(5) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und / oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und / oder die Einhaltung der Weisungen durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

§ 3 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten bestellt hat. Dessen Kontaktdaten lauten:
Herr Ulrich Wurmbach, Buhl Data Service GmbH, Am Siebertsweiher 3/5, 57290 Neunkirchen, datenschutz@buhl-data.com

(2) Der Auftragnehmer sichert im Bereich der auftragsgemässen Verarbeitung von personenbezogenen Daten die vertragsmässige und gesetzeskonforme Abwicklung aller vereinbarten Massnahmen zu.

(3) Der Auftragnehmer ist verpflichtet, das Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die im Auftrag des Auftraggebers verarbeitet werden, im jeweils erforderlichen Mass gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Aufragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine von dem Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstösst. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden gesetzlich mitteilungspflichtigen Verstoss gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und / oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist. Er wird den Auftraggeber unverzüglich über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde informieren. Dies gilt auch, soweit eine zuständige Behörde beim Auftragnehmer ermittelt.

(6) Es ist bekannt, dass Informationspflichten im Falle des Abhandenkommens oder der unrechtmässigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind diese Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmässigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Massnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

(7) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(8) Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(9) Der Auftragnehmer ist zur Begründung von Unterauftragsverhältnissen nur mit schriftlicher Zustimmung des Auftraggebers berechtigt. Der Auftragnehmer hat in diesem Falle sicherzustellen, dass die vereinbarten Regelungen auch gegenüber dem Unterauftragnehmer gelten. Er hat die Einhaltung dieser Pflichten regelmässig zu überprüfen. Die Weiterleitung von Daten ist nicht zulässig, bevor der Unterauftragnehmer die Verpflichtungen erfüllt hat. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind

solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmassnahmen zu ergreifen.

§ 4 Datengeheimnis

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses verpflichtet.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweiligen geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer gewährleistet, dass die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie massgeblichen Bestimmungen des Datenschutzes vertraut gemacht werden und diese auf das Datengeheimnis verpflichtet werden.

§ 5 Technische und organisatorische Massnahmen zur Datensicherheit

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Massnahmen (siehe hierzu Anlage 1), die zur Wahrung der anzuwendenden Datenschutzvorschriften erforderlich sind:

(1) Zutrittskontrolle
Der Auftragnehmer trifft alle erforderlichen Massnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

(2) Zugangskontrolle
Der Auftragnehmer trifft alle erforderlichen Massnahmen um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies umfasst neben der Verwendung von dem Stand der Technik entsprechender Verschlüsselungsverfahren.

(3) Zugriffskontrolle
Der Auftragnehmer gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugangsberechtigung 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. Er trifft alle hierzu erforderlichen Massnahmen einschliesslich der Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

(4) Weitergabekontrolle
Der Auftragnehmer gewährleistet, 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. Er trifft alle hierzu erforderlichen Massnahmen einschliesslich der Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

(5) Eingabekontrolle
Der Auftragnehmer gewährleistet, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Er trifft alle hierzu erforderlichen Massnahmen.

(6) Auftragskontrolle
Der Auftragnehmer gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Er trifft alle hierzu erforderlichen Massnahmen.

(7) Verfügbarkeitskontrolle
Der Auftragnehmer gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Er trifft alle hierzu erforderlichen Massnahmen.

(8) Trennungskontrolle
Der Auftragnehmer gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Er trifft alle hierzu erforderlichen Massnahmen. Der Auftragnehmer hat dem Auftraggeber auf dessen Anforderung die Beschreibung der konkreten Umsetzung dieser technischen und organisatorischen Massnahmen zur Datensicherheit gemäss Anlage 1 in der jeweils aktuellen Fassung in Form eines internen Verfahrens in schriftlicher Form zur Verfügung zu stellen.

§ 6 Folgen der Vertragsbeendigung

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemässe Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Die Löschung ist durch den Auftragnehmer in geeigneter Weise zu dokumentieren, das Protokoll der Löschung ist dem Auftraggeber auf Anforderung vorzulegen.

§ 7 Vertraulichkeit, Informationspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden.

(2) Soweit dieser Vertrag keine Regelungen enthält, gelten die allgemeinen gesetzlichen Bestimmungen.

(3) Die Nichtigkeit oder Unwirksamkeit einzelner Bestimmungen dieses Vertrags berührt die Gültigkeit der übrigen Bestimmungen nicht. Die mangelhafte Bestimmung gilt als durch eine solche ersetzt, deren wirtschaftlicher und juristischer Sinn ihr möglichst nahekommt.

§ 8 Schlussbestimmungen

(1) Vertragsänderungen bedürfen zu ihrer Wirksamkeit der Schriftform. Das Gleiche gilt für den Verzicht auf das Schrifterfordernis.

(2) Soweit dieser Vertrag keine Regelungen enthält, gelten die allgemeinen gesetzlichen Bestimmungen.

§ 9 Anwendbares Recht

Es findet ausschliesslich Schweizer Recht unter Ausschluss des UN-Kaufrechts Anwendung. Erfüllungsort und Gerichtsstand ist Tägerwilen.

cobra computer's brainware AG
High-Tech-Center 2
Bahnstrasse 1
8274 Tägerwilen

Stand: November 2017

Die Allgemeinen Geschäftsbedingungen zur cobra PrivateCloud finden Sie auf www.cobraag.ch

cobra®
CRM

Anlage 1

Beschreibung der konkreten Umsetzung der technischen und organisatorischen Massnahmen zur Datensicherheit gemäss § 5

(1) Zutrittskontrolle
Um Unbefugten den Zutritt zu den Datenverarbeitungsanlagen zu verwehren, werden folgende Massnahmen eingesetzt:

- Zutrittskontrollsystem zu allen Gebäuden mittels Transponderchip
- Videoüberwachung am Empfang
- Alarmanlage/Schliesssystem mit Codesperre
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Zusätzliche Sicherheitsschlösser und Berechtigungen zu Serverräumen

(2) Zugangskontrolle
Die Nutzung der Datenverarbeitungssysteme durch Unbefugte wird wirkungsvoll verhindert durch:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Einsatz von VPN-Technologie
- Authentifikation mit Benutzername / Passwort
- Zwang zur regelmässigen Passwortänderungen
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von zentraler Mobile-Device-Administrations-Software (z.B. zum Ändern von Passwörtern)
- Prüfung durch unabhängige IT-Spezialisten

(3) Zugriffskontrolle
Es werden folgende Möglichkeiten genutzt, 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:

- Nutzung eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Trennung von Berechtigungsanforderung und -vergabe
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- Sichere Vernichtung von Datenträgern durch Zerstörung

(4) Weitergabekontrolle
Es wird gewährleistet, 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, durch

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Sichere Verschlüsselung
- Protokollierung

(5) Eingabekontrolle
Es wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

(6) Auftragskontrolle
Es werden Massnahmen ergriffen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können durch

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Kontrolle der Vertragsausführung

(7) Verfügbarkeitskontrolle
Personenbezogene Daten werden gegen zufällige Zerstörung oder Verlust geschützt durch

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

(8) Trennungskontrolle
Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können mit folgenden Festlegungen:

- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)