Bastian Wetzel

Dokumentation der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes bei Collmex

Verteiler: Alle Mitarbeiter sowie interessierte Kunden der Collmex GmbH, Anlage 1 zum Vertrag zur Nutzung einer Online-Unternehmenssoftware

Inhaltsverzeichnis:

Einleitung

Als Auftragsdatenverarbeiter für betriebliche Anwendungen (Buchhaltung, Auftragsverarbeitung, Warenwirtschaft usw.) hat die Collmex GmbH, im Folgenden Collmex genannt, eine besondere Verantwortung für die Daten seiner Kunden. Ein Verlust dieser Daten hätte weit reichende Folgen - sowohl für unsere Kunden als auch für Collmex selbst. Aus diesem Grund hat Collmex die erforderlichen technischen und organisatorischen Maßnahmen getroffen, diese Daten nach dem aktuellen Stand der Technik zu schützen.

Diese Dokumentation beschreibt die technischen und organisatorischen Maßnahmen zur Einhaltung und Umsetzung des Datenschutzes bei Collmex. Die Dokumentation richtet sich nicht nur an alle Mitarbeiter von Collmex, sondern explizit auch an alle Kunden und Interessenten.

Jeder Kunde von Collmex ist laut §11 BDSG dazu verpflichtet, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes zu überzeugen. Grundlage hierfür bildet diese Dokumentation. In der Anlage zu §9 Satz 1 BDSG sind die erforderlichen Maßnahmen konkretisiert. Um Kunden und Interessenten eine Prüfung gemäß §11 BDSG zu erleichtern, richtet sich die Gliederung dieser Dokumentation nach der Anlage zu §9 Satz 1 BDSG.

Datenkategorien

Es gibt zwei Kategorien von personenbezogenen Daten: Zum einen die betrieblichen Daten der Kunden, im Folgenden **Kundendaten** genannt. Die Erhebung, Verarbeitung und Nutzung dieser Kundendaten erfolgt ausschließlich durch die Kunden selbst über das Internet über das https Protokoll. Im Rahmen der technischen Wartung besteht jedoch die Möglichkeit des Zugriffs auf die Kundendaten durch Collmex und durch den Rechenzentrumsbetreiber. Nur die Kundendaten sind Gegenstand der Auftragsdatenverarbeitung.

Die zweite Datenkategorie sind die zur Verwaltung und Abrechnung erforderlichen Daten (Name und Anschrift des Kunden, genutzte Programmversion usw.), Adressdaten von Interessenten, Mitarbeitern sowie Bewerberdaten sowie Daten von Lieferanten. Diese Daten werden im Folgenden **Verwaltungsdaten** genannt. Die Erhebung, Verarbeitung und Nutzung der Verwaltungsdaten erfolgt durch Collmex oder auch durch die Kunden selbst über eine Verwaltungssoftware und das https Protokoll. Im Rahmen der technischen Wartung besteht jedoch die Möglichkeit des Zugriffs auf die Verwaltungsdaten durch den Rechenzentrumsbetreiber.

Zutrittskontrolle

Über die Zutrittskontrolle wird Unbefugten der Zutritt verwehrt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Bei den Räumlichkeiten, in denen sich die Datenverarbeitungsanlagen befinden, muss unterschieden werden zwischen dem Rechenzentrum, normalen Büroräumen und dem Backup-Rechenzentrum.

Rechenzentrum

Im Rechenzentrum befinden sich die Server, auf denen sowohl die Kundendaten als auch die Verwaltungsdaten zentral gespeichert und verarbeitet werden. Die Zutrittskontrolle zu den Servern ist deshalb von besonderer Bedeutung.

Das Rechenzentrum wird nicht von Collmex selbst, sondern von der Host Europe GmbH betrieben. Mit dem Rechenzentrumsbetreiber besteht eine Vereinbarung zur Auftragsdatenverarbeitung. Das Rechenzentrum wurde vom eco-Verband mit der Bestnote von fünf Sternen zertifiziert und gilt damit eines der sichersten in Deutschland.

Der Zugang zum Rechenzentrum wird durch den Rechenzentrumsbetreiber kontrolliert. Im Rechenzentrum hat die Zutrittskontrolle einen sehr hohen Standard, welcher im Rahmen des Data Center Star Audits vom eco-Verband überprüft wurde und umfasst unter Anderem folgende Merkmale:

- Prozess benutzerbezogener Authentifizierung (Biometrie oder geistiges Identifikationsmerkmal)
- Zugang zum Rechenzentrum über mind. 2 Türsysteme
- Vereinzelungsanlage (Kundenzutritt) oder Schleusensystem
- Physikalischer Zugangsschutz mit Logging (Stahltüren/Sicherheitsschlösser/fensterloser Raum oder gesicherte Fenster) und eine Alarmierung/Einbruchssicherung

Büroräume

Büroräume sind zum einen die Räumlichkeiten am Firmensitz der Collmex GmbH in Saarbrücken. Zum anderen ist es einzelnen Mitarbeitern auch gestattet, mit mobilen Rechnern von anderen Orten aus zu arbeiten (z.B. von zu Hause aus). In Büroräumen befinden sich normalerweise keine unverschlüsselten Kunden- oder Verwaltungsdaten. Einzige Ausnahme ist eine temporäre Kopie der Daten einzelner Kunden für spezielle Support-Aufgaben (z.B. Fehlersuche mittels Debugger, s. Zugriffskontrolle).

Da in Büroräumen keine unverschlüsselten Kunden- oder Verwaltungsdaten gespeichert werden, ist für die Büroräume keine spezielle Zutrittskontrolle erforderlich. Die Sicherungsmechanismen entsprechen denen normaler gewerblich genutzter Räumlichkeiten.

Backup-Rechenzentrum

Als zusätzliches Backup-Rechenzentrum wird ein räumlich getrenntes Rechenzentrum genutzt. In das Backup-Rechenzentrum werden die gepackten und verschlüsselten Kunden- und Verwaltungsdaten jede Nacht übertragen und ausschließlich verschlüsselt gespeichert. Das Kennwort zur Entschlüsselung ist nur Mitgliedern der Geschäftsführung von Collmex bekannt. Ein Zugriff auf die Daten von anderen Personen kann ausgeschlossen werden. Für das Backup-Rechenzentrum ist deshalb keine spezielle Zutrittskontrolle erforderlich.

Zugangskontrolle

Über die Zugangskontrolle wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Server im Rechenzentrum

Nur auf den Servern im Rechenzentrum sind die Kunden- und Verwaltungsdaten zentral und unverschlüsselt gespeichert. Die Zugangskontrolle zu diesen Servern ist deshalb von besonderer Bedeutung.

Die Server im Rechenzentrum verfügen zur Administration über entsprechende Benutzerkonten. Die Administration der Server erfolgt über das Internet über ein verschlüsseltes Protokoll. Die Kennwörter für diese Benutzerkonten sind nur der Geschäftsführung bekannt. Zusätzlich gibt es noch ein Administrator-Konto für den Zugriff von Mitarbeitern des Rechenzentrums, welches jedoch nur im Bedarfsfall aktiviert wird.

Um unautorisierten Zugang zu verhindern, sind die Rechner zudem über zwei hintereinander geschaltete Firewalls geschützt. Bei der ersten Firewall handelt es sich um eine externe hardwarebasierte Cisco-Firewall, bei der zweiten Firewall um eine softwarebasierte Firewall. Beide Firewalls sind so konfiguriert, dass nur der Datenverkehr zugelassen ist, der für den Betrieb der Software zwingend erforderlich ist.

Zugang zu anderen Datenverarbeitungsanlagen

Der Zugang zu den Rechnern in den Büroräumen wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter ein eigenes Benutzerkonto sowohl für den lokalen Rechner, als auch für die Verwaltungssoftware, mit deren

Hilfe auf die Kunden- und Verwaltungsdaten im Rahmen des Supports kontrolliert zugegriffen werden kann (s. Zugriffskontrolle).

Zugang zu dem Server im Backup-Rechenzentrum haben nur Mitglieder der Geschäftsführung.

Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, 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.

Zugriff auf Kundendaten durch Support-Mitarbeiter

Support-Mitarbeiter haben immer nur Zugriff auf die Kundendaten, die sie im Rahmen ihrer Tätigkeit gerade benötigen. Die Möglichkeit des gleichzeitigen Zugriffs auf alle Kundendaten ist den Mitgliedern der Geschäftsführung vorbehalten.

Zur Kontrolle des Zugriffs auf die Kundendaten verfügt jedes Kundenprogramm über einen eigenen Service-Benutzer. Benutzernamen und Kennwörter der Service-Benutzer sind in der Verwaltungssoftware gespeichert und können vom Kunden nicht geändert werden. Support-Mitarbeiter mit Zugang zur Verwaltungssoftware können den Service-Benutzer und das Kennwort jederzeit einsehen und sich über die Verwaltungssoftware am Kundenprogramm anmelden. Der Support-Mitarbeiter kann über einen Internet-Browser das Programm genau so benutzen, wie es auch dem Kunden selbst möglich ist.

Der Service-Benutzer ist normalerweise gesperrt und kann nur durch den Kunden selbst entsperrt werden. Durch das Entsperren des Service-Benutzers gewährt der Kunde dem Support-Mitarbeiter Zugang zu seinen Daten. Sperrt der Kunde den Service-Benutzer nach Abschluss der Service-Arbeiten nicht selbst, so wird der Service-Benutzer spätestens nach fünf Tagen automatisch gesperrt. *Ausnahme*: Bei Endkunden, die über Wiederverkäufer abgerechnet werden (z.B. Steuerberater), ist der Service-Benutzer immer entsperrt, um dem Wiederverkäufer jederzeit Zugriff auf das Programm des Endkunden zu ermöglichen.

Für einige speziellere Support-Aufgaben ist es erforderlich, auf technischer Ebene auf die Daten zuzugreifen (z.B. zur Fehlersuche mittels Debugger). In diesem Fall meldet sich ein Mitglied der Geschäftsführung auf dem Server im Rechenzentrum an und stellt die Daten des betroffenen Kunden dem

Support-Mitarbeiter als lokale Kopie zur Verfügung. Die Mitarbeiter sind angewiesen, direkt nach Abschluss der Service-Arbeiten die lokale Datenkopie wieder zu löschen.

Collmex hat mit jedem Mitarbeiter eine schriftliche Vereinbarung über die sicher gestellt wird, dass Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Zugriff auf Sicherungskopien

Sicherungskopien werden grundsätzlich mit einem gängigen und als sicher geltenden Verfahren auf den Servern im Rechenzentrum verschlüsselt. Das Kennwort zur Entschlüsselung der Sicherungskopien ist nur den Mitgliedern der Geschäftsführung von Collmex bekannt. So ist sicher gestellt, dass nur befugte Personen Zugriff auf die Kunden- und Verwaltungsdaten haben, auch wenn unbefugte Personen Zutritt oder Zugang zu einer Sicherungskopie erlangen sollten.

Weitergabekontrolle

Die Weitergabekontrolle 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.

Die Weitergabekontrolle wird bei Collmex durch den einzigen Speicherort der Kunden- und Verwaltungsdaten im Rechenzentrum und die restriktive Zutritts- und Zugangskontrolle zu diesem Speicherort sichergestellt. Das unbefugte lesen, kopieren, verändern oder entfernen von im Rechenzentrum gespeicherten Daten durch den Rechenzentrumsbetreiber ist vertraglich ausgeschlossen.

Die Daten werden nur in verschlüsselter Form nach außerhalb des Rechenzentrums übertragen oder in verschlüsselter Form außerhalb des Rechenzentrums gespeichert. Das Kennwort zur Entschlüsselung der Daten ist nur den Mitgliedern der Geschäftsführung bekannt, so dass eine unberechtigte Weitergabe ausgeschlossen werden kann.

Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Eingabekontrolle wird bei Collmex zum einen über Protokolldateien gewährleistet. Die Protokolldateien sind Textdateien und Teil der Kunden- bzw. Verwaltungsdaten. Sie sind nur nach Anmeldung auf dem Server im Rechenzentrum einsehbar oder nach auspacken der verschlüsselten Sicherungen. In den Protokolldateien sind sämtliche Eingaben aufgezeichnet, die Kunden oder Mitarbeiter über das https Protokoll in Kunden- oder Verwaltungsdaten gemacht haben. Die Aufbewahrungszeit für die Protokolle beträgt mindestens ein Jahr.

Zum anderen haben Kunden die Möglichkeit in ihrem Programm selbst zu sehen, welcher Benutzer zu welchem Zeitpunkt einen Datensatz (z.B. Kunde) zuletzt geändert hat.

Auftragskontrolle

Die Auftragskontrolle stellt sicher, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Als einziger Datenverarbeiter mit möglichem Zugang zu den Daten ist der Rechenzentrumsbetreiber Host Europe beauftragt. Mit dem Rechenzentrumsbetreiber besteht eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung über die sicher gestellt ist, dass die Daten nur entsprechend den Weisungen von Collmex verarbeitet werden. Eine Nutzung oder Weitergabe der Daten durch Mitarbeiter des Rechenzentrums ist vertraglich ausgeschlossen.

Support-Aufträge werden beim Rechenzentrumsbetreiber nur durch Mitarbeiter der Geschäftsführung von Collmex in das Auftragssystem des Rechenzentrumsbetreibers eingestellt. Die Aufträge von Collmex an das Rechenzentrum liegen damit schriftlich vor und können nachträglich überprüft werden.

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Verfügbarkeit der Daten wird durch ein mehrstufiges Sicherungskonzept gewährleistet. Die erste Stufe bilden die Server selbst mit ihren gespiegelten Festplatten (RAID). Der Ausfall einer Festplatte hat damit keinen Datenverlust zur Folge. Defekte Festplatten können im laufenden Betrieb ausgetauscht werden (Hot-Plug). Der Status des RAID-Systems wird regelmäßig überwacht und bei einer Störung wird der Rechenzentrumsbetreiber mit dem Austausch der defekten Festplatte beauftragt.

Als zweite Sicherungsstufe werden die Daten jede Nacht komprimiert, verschlüsselt und auf ein dafür vorgesehenes Backup-System des Rechenzentrumsbetreibers kopiert.

In der dritten Sicherungsstufe wird die verschlüsselte Datenkopie zusätzlich im räumlich getrennten Backuprechenzentrum archiviert. Optional wird die Sicherungskopie zusätzlich in den Büroräumen gespeichert.

Im Rechenzentrum bieten vollklimatisierte Sicherheitsräume Schutz vor Gas, Wasser und Feuer. Der zusätzliche Speicherort im Backuprechenzentrum sichert darüber hinaus auch größte anzunehmende Unfälle ab, wie z.B. einen Flugzeugabsturz in das erste Rechenzentrum.

Getrennte Verarbeitung

Die getrennte Verarbeitung gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der getrennten Verarbeitung kommt bei Collmex eine besondere Bedeutung zu, da die Daten vieler Kunden gleichzeitig auf einem Server verarbeitet werden.

Zur Gewährleistung der getrennten Verarbeitung sind die Daten unterschiedlicher Kunden auf dem Server nach Verzeichnissen getrennt gespeichert, d.h. für jeden Kunden existiert ein eigenes Verzeichnis, in dem nur die Daten dieses einen Kunden gespeichert sind.

Für jeden Kunden existiert eine eigene Datenbank und ein eigener Betriebssystem-Prozess, in dem nur die Daten dieses einen Kunden verarbeitet werden. Daten unterschiedlicher Kunden werden nie gemeinsam in einem Betriebssystem-Prozess verarbeitet oder in einer gemeinsamen Datenbank verwaltet, sondern sind stets strikt getrennt.