Technische und organisatorische Maßnahmen der ATOSS Aloud GmbH

Anlage 1 zum AVV der ATOSS Aloud GmbH

Vertraulichkeit

Zutrittskontrolle

Der Unternehmenssitz befindet sich in der 3. Etage der Rosenheimer Str. 116b, 81669 München.

Der Zutritt erfolgt über mechanische Schlüssel. Diese werden personenspezifisch durch den Standortverantwortlichen vergeben. Die Vergabe wird in einem Schlüsselbuch protokolliert.

Der Zutritt betriebsfremder Personen (etwa Besucherinnen und Besucher) zu den Büroräumen ist wie folgt beschränkt:
Betriebsfremde Personen klingeln an der Eingangstür. Nach einem ersten Gesprächskontakt über die Fernsprechanlage wird die Tür durch einen zuständigen Mitarbeiter geöffnet. Der Zugang zu den Büroräumen und der Aufenthalt im Büro erfolgt nur in deren Begleitung.

Ein Sicherheitsdienst ist außerhalb der Geschäftszeiten beauftragt.

Zugangskontrolle

Benutzerzugänge zu den Arbeitsplatzrechnern werden nur personenbezogen vergeben.

Direkter Zugang zu Servern im Internet auf ist ausschließlich verschlüsselt und mit personenbezogenen digitalen Schlüsseln möglich. Server im Internet sind mit einer aktuellen Firewall geschützt.

Zugang auf Rechner innerhalb des Bürogebäudes von außerhalb des Bürogebäudes sind nicht vorgesehen. Zugang auf Server im Internet von außerhalb des Bürogebäudes, z.B. vom Heimarbeitsplatz ist möglich. Der Zugang kann aber auch hier ausschließlich verschlüsselt und persönlich authentifiziert erfolgen (HTTPS/SSH, Passwort und/oder Private Key).

Die Passwörter zu den Benutzerkonten auf den Arbeitsplatzrechnern werden vom jeweiligen Mitarbeiter selbst vergeben und sind nur diesem bekannt.

Passwörter für die Arbeitsplatzrechner müssen mindestens aus 10 Zeichen bestehen und mindestens einen Buchstaben, eine Zahl und ein Sonderzeichen enthalten. Dies wird durch eine lokale Richtlinie des Betriebssystems sichergestellt.

Die Mitarbeiter sind verpflichtet, Passwörter ausschließlich in einem dafür vorgesehenen Passwortspeicher zu sichern. Dieser verwendet Industriestandards zur Verschlüsselung der Daten.

Die Festplatten der Arbeitsplatzrechner sind verschlüsselt, aktuell durch macOS mit einer XTS-AES-128-Verschlüsselung mit einem 256-Bit-Schlüssel.

Die Mitarbeiter sind angehalten, bei jedem Verlassen des Arbeitsplatzes ihren Computer zu sperren. Danach ist eine Passworteingabe zur Entsperrung notwendig.

Zugriffskontrolle

Mitarbeiter bekommen nur Zugriff auf ihren eigenen Arbeitsplatzrechner bzw. auf Server und Dienste im Internet, die für die Arbeit in ihrer jeweiligen Arbeitsbereich relevant sind. Die Zugriffskongfolle folgt dabei der Organisations-/Abteilungsstruktur.

Zugriff auf Dokumente und Kommunikations-Informationen sind nur nach entsprechender personenbezogenen Autorisierung möglich.

Die Entwicklungsabteilung prüft in regelmäßigen Abständen die Rechte- und Benutzerstruktur und reduziert den Zugriff so weit wie möglich. Beim Ausscheiden oder dem internen Wechsel eines Mitarbeiters erfolgt diese Prüfung ebenfalls nach entsprechender Mitteilung durch die Personalabteilung.

Datenträgerkontrolle

Nicht mehr benötigte elektronische Datenträger (Festplatten, CD-ROMs, DVDs, USB-Sticks), auf denen Auftragsdaten gesichert sind, werden wie folgt entsorgt:

Elektronische Datenträger werden durch einen externen Entsorgungsdienstleister physisch vernichtet. Die Löschung und Vernichtung erfolgt in Übereinstimmung mit internen Aufbewahrungsrichtlinien, gesetzlichen Aufbewahrungspflichten und anderen einschlägigen gesetzlichen Bestimmungen und betriebsinternen Regelungen. Vor jeder Vernichtung und Löschung von Datenträgern wenden sich Mitarbeiter stets an die IT-Abteilung des Auftragnehmers. Die Übergabe erfolgt dabei über den Mutterkonzern ATOSS Software AG.

Nicht mehr benötigte Unterlagen mit personenbezogenen Daten des Auftraggebers (Akten, Schriftwechsel etc.) im Unternehmen werden wie folgt entsorgt:
Die Vernichtung erfolgt durch einen Entsorgungsdienstleister. Hierzu sind in allen Geschäftsstellen und Konzernunternehmen verschlossene „Datentonnen“ aufgestellt, die regelmäßig sowie ggf. zusätzlich bei Erforderlichkeit geleert werden.

Mit dem externen Entsorgungsdienstleister ist ein den gesetzlichen Vorgaben entsprechender Vertrag zur Auftragsdatenverarbeitung geschlossen worden.

Trennungskontrolle

Nach Möglichkeit werden nur die jeweiligen persönlichen Daten in für die jeweiligen Einsatzgebiete spezialisierten Anwendungen gespeichert, z.B. Bezahldaten nur im Payment-System, nicht aber im CRM.

Integrität

Weitergabekontrolle

Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen .

Weitergabe von Daten erfolgt generell verschlüsselt über Netzwerkprotokolle, z.B. per HTTPS/SSH/SCP/SFTP. Dies kann aber nicht in allen Fällen praktikabel angewendet werden, z.B. beim Versenden von Emails.

Weitergabe von Daten auf physischen Datenträgern wird generell vermieden.

Eingabekontrolle

Präferiert werden Systeme eingesetzt, die jede Datenänderung protokolliert. Allerdings bietet das nicht jedes unserer eingesetzten Systeme an.

Das Risiko (unbeabsichtigte) Überschreiben von personenbezogenen Daten wird durch die gezielte Vergabe von Berechtigungen für dedizierte Systeme gemindert. Zusätzlich beugen regelmäßig erstellte Backups einem Überschreiben von Auftragsdaten vor (siehe auch “Verfügbarkeitskontrolle”).

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

In den Büroräumen der ATOSS Aloud GmbH werden Daten nur auf den Arbeitsplatzrechnern der Mitarbeiter verarbeitet. Das eingesetzte Emailprogramm bietet aktuelle SPAM-Filtermechanismen. Das eingesetzte Betriebssystem enthält einen Virenscanner / Malwareschutz, der vom Hersteller regelmäßig aktualisiert wird.

Es gibt neben den Arbeitsplatzrechnern keine lokale Infrastruktur zur Datenverarbeitung. Jegliche weitere Datenverarbeitung findet ausschließlich auf Hardware von Unterauftragnehmern in deren Datencentern statt. Mit allen diesen Unterauftragnehmern wurden AVV abgeschlossen.

Die Produktivsysteme laufen auf physischen Servern mit RAID-Spiegelungskonzepten bzw. auf virtualisierten Servern mit entsprechendem Redundanzkonzepten.

Es werden mehrfach täglich automatische Sicherungskopien/Backups der Datenbanken mit allen Crewmeister- Kundendaten erstellt. Die Backups werden verschlüsselt digital zu einem Drittanbieter transferiert, der die Daten physisch getrennt von denen der Produktivsysteme speichert. Die Daten werden ca. 14 Tage aufbewahrt und danach gelöscht.

Es gibt ein Konzept zur Rekonstruktion dieser Datenbestände und zudem eine regelmäßige stichprobenhafte Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können. Dadurch wird rasche Wiederherstellbarkeit dieser Daten gewährleistet.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Überprüfung der Maßnahmen

Das Betriebssystem auf den Arbeitsplatzrechnern wird automatisch zeitnah beim Vorliegen von neuen Versionen aktualisiert.

Für Server bei Unterauftragnehmern, die unter der Kontrolle der ATOSS Aloud GmbH sind, wird das Betriebssystem und die Firewall regelmäßig auf neue Versionen hin geprüft und aktualisiert.

Die in der Crewmeister-Anwendung verwendeten Bibliotheken und Komponenten von Drittanbietern werden vor der Öffentlichung einer neuen Version gegenüber bekannten Sicherheitslücken geprüft. Liegt eine solche vor, wird keine neue Version ausgespielt, bis eine unbedenkliche Fassung der Bibliothek verwendet wird.

Die Qualitätssicherungsprozesse in der Softwareentwicklung basieren auf etablierten und vereinbarten Standards wie z.B. Code Reviews und Akzeptanztests, wodurch auch potenzielle Datenschutzrisiken regelmäßig berücksichtigt und überprüft werden.

Datenschutzfreundliche Voreinstellungen

Die Software-Lösungen des Auftragnehmers aktualisieren sich per Voreinstellung automatisch, so dass etwaige datenschutzrechtliche Risiken schnell und unkompliziert geheilt und in einer neuen Fassung an alle Anwender verteilt werden können.

Einzelne Funktionen der Software-Lösungen des Auftragnehmers sind deaktivierbar, ohne dass sich die Deaktivierung auf die Funktionalität der Software-Lösungen im Übrigen auswirkt. Die Software-Lösungen bestehen aus unterschiedlichen Modulen, die nur teilweise aufeinander aufbauen und deren Funktionalität nur teilweise von der eines anderen Moduls abhängen.

Auftragskontrolle

Durch schriftliche Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 53 BDSG n.F.) sowie wiederkehrende Belehrungen im Rahmen regelmäßiger Schulungen zum Datenschutz wird sichergestellt, dass Mitarbeiter Auftragsdaten des Auftraggebers nur entsprechend der Anweisungen des Auftraggebers verarbeiten.

Zwischen dem Auftragnehmer und seinen Unterauftragnehmern werden Verträge über die Auftragsverarbeitung gemäß den Anforderungen nach Art. 28 DS-GVO bzw. § 62 Abs. 3 BDSG n.F. geschlossen. In den Verträgen ist insbesondere festgelegt, dass der Auftraggeber weisungsbefugt ist und die Mitarbeiter des Unterauftragnehmers auf das Datengeheimnis verpflichtet sind. So ist sichergestellt, dass auch Unterauftragnehmer Auftragsdaten des Auftraggebers nur im Auftrag und entsprechend der Anweisungen des Auftraggebers verarbeiten. Der Auftraggeber hat Kenntnis der eingesetzten Unterauftragnehmer und genehmigt diese im Rahmen der Vereinbarung der AVV.

Es wurde schriftlich ein Konzern-Datenschutzbeauftragter (BSD) bestellt:

Dr. Maximilian Hoffmann

Stand: 01.01.2020

089 / 42771 – 125
maximilian.hoffmann@atoss.com

Der DSB hat nachweislich an einem anerkannten Lehrgang zum Datenschutzbeauftragten teilgenommen. Kopien der Bestellungsurkunde und des Fachkundenachweises sind vorhanden und können dem Auftraggeber auf Verlangen vorgelegt werden.

Hinweis: Im Falle von Änderungen der getroffenen und dokumentierten technischen und organisatorischen Maßnahmen (Anlage 1 zur Vereinbarung zur Auftragsverarbeitung) wird dem Auftraggeber die jeweils mit aktuellem Tagesdatum versehene Fassung der Anlage 1 auf geeignete Weise zur Verfügung gestellt, z.B. auf einem über die Website des Auftragnehmers zugänglichen Online-Portal. Der Auftraggeber ist verpflichtet, sich regelmäßig über die aktuelle Fassung der Anlage 1 zu informieren.