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

Actionbound GmbH, nachfolgend “Actionbound” genannt.

Zutrittskontrolle

Verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben.

Für die Räumlichkeiten der Datenverarbeitungsanlagen muss zwischen Rechenzentrum und Büroräumen unterschieden werden.

Rechenzentrum

Die Rechenzentren werden in Deutschland von Hetzner Online GmbH, 1&1 Internet SE und Amazon Web Services, Inc. betrieben. Amazon Web Services, Inc. hat vertraglich zugesichert, alle Daten ausschließlich in Rechenzentrum im Großraum Frankfurt/Main zu verarbeiten. Mit den Rechenzentrumsbetreibern besteht jeweils eine Vereinbarung zur Auftragsdatenverarbeitung. Der Zugang zum Rechenzentrum wird durch den Rechenzentrumsbetreiber kontrolliert. Der übliche, hohe Industriestandard zur Zutrittskontrolle wurde Actionbound vertraglich zugesichert und bei der Auswahl der Dienste berücksichtigt. Die Dokumentation kann auf Nachfrage von Actionbound versandt werden.

Büroräume

Büroräume sind die Räumlichkeiten am Firmensitz von Actionbound in Hohenpeißenberg und im Büro Berlin. Zum anderen ist es einzelnen Mitarbeitern, die sich als besonders vertrauenswürdig erwiesen haben, auch gestattet, von anderen Orten aus zu arbeiten (z. B. auf einer Dienstreise). Mitarbeitern mit Leitungsfunktion, die sich als besonders zuverlässig erwiesen haben, wird im Einzelfall gestattet, aus einem abschließbaren häuslichen Arbeitszimmer zu arbeiten. Alle Mitarbeiter sind schriftlich zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung verpflichtet. Es wird durch entsprechende Weisungen an alle Mitarbeiter sichergestellt, dass sich in Büroräumen grundsätzlich keine unverschlüsselten Kunden- oder Verwaltungsdaten befinden und keine unverschlüsselten Kunden- oder Verwaltungsdaten aus den Büroräumen mitgenommen werden.

Daher ist für die Büroräume keine spezielle Zutrittskontrolle erforderlich. Die Sicherungsmechanismen entsprechen denen normaler gewerblich genutzter Räumlichkeiten, d. h. Türschloss mit protokollierter Schlüsselvergabe, Jalousien.

Zugangskontrolle

Verhindern, dass Unbefugte Datenverarbeitungsanlagen nutzen können.

Rechenzentren

Auf den Servern in den Rechenzentren sind die Kunden- und Verwaltungsdaten zentral 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 mit Zugang über 4096 bit RSA Schlüsseln. Diese Schlüssel sind nur der Geschäftsführung bekannt und werden regelmäßig geändert.

Rechner der Mitarbeiter

Der Zugang zu den Rechnern der Mitarbeiter 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). Die Mitarbeiter sind dazu verpflichtet, Passwörter laut Empfehlung des Bundesamts für Sicherheit in der Informationstechnik zu benutzen. Die Übertragung zwischen den Rechenzentren zu den Rechnern der Mitarbeiter ist verschlüsselt.

Zugriffskontrolle

Gewährleisten, dass nur Berechtigte auf Daten zugreifen können und diese nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können.

Der Zugriff auf Kundendaten ist nur geschulten Mitarbeitern von Verkauf, Buchhaltung und Support, sowie der Geschäftsführung möglich. Dies wird durch Vergabe von Berechtigungen durch die Geschäftsführung an die Mitarbeiter sichergestellt.

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

Weitergabekontrolle

Gewährleisten, dass Daten bei der elektronischen Übertragung/Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Weitergabekontrolle wird bei Actionbound durch die Speicherorte der Kunden- und Verwaltungsdaten in den Rechenzentren und die restriktive Zutritts- und Zugangskontrolle zu

diesen Speicherorten sichergestellt. Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von im Rechenzentrum gespeicherten Daten durch den Rechenzentrumsbetreiber ist vertraglich ausgeschlossen. Zur Übertragung sind die Daten – wie oben unter Zugangskontrolle angegeben – verschlüsselt.

Eingabekontrolle

Gewährleisten, dass nachträglich überprüft werden kann, ob und wer Daten verändert oder entfernt hat.

Um die Eingabekontrolle sicherzustellen, werden bei Actionbound die Eingaben, die die Mitarbeiter in der Kundenverwaltung durchführen, protokolliert. Mit dieser Protokolldatei kann jederzeit nachvollzogen werden, welche Eingaben oder Änderungen durch welchen Mitarbeiter vorgenommen wurden. Duplikate der Protokolldatei werden georedundant gesichert.

Auftragskontrolle

Gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können.

Mit allen Datenverarbeitern besteht eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung über die sichergestellt ist, dass die Daten nur entsprechend den Weisungen von Actionbound verarbeitet werden. Eine Nutzung oder Weitergabe der Daten durch Mitarbeiter der Datenverarbeiter ist vertraglich ausgeschlossen.

Verfügbarkeitskontrolle

Gewährleisten, dass 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 parallel auf einem zweiten Rechner im Rechenzentrum vorgehalten, um bei einem Ausfall des Primärsystems unverzüglich Zugang zu erhalten.

Als dritte Sicherungsstufe werden die Daten täglich komprimiert und nach dem etablierten Stand der Technik verschlüsselt in ein separates, örtlich getrenntes Backup-Rechenzentrum übertragen.

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

Getrennte Verarbeitung

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Daten, die zu unterschiedlichen Zwecken erhoben werden (z. B. Lizenzen, Bound-Erstellung, Bound-Ergebnisse), werden in unterschiedlichen Datenbanksammlungen gespeichert.
Die Test-, Qualitätssicherungs- und Produktionssysteme laufen auf unterschiedlichen Instanzen mit komplett getrennten Datenbanken. Die Datenbanken sind logisch von der Applikationsschicht getrennt. Die Synchronität der Datenbanken wird durch Replikation sichergestellt.

Stand vom 16.12.2019