5.1.1 Datensicherungsrichtlinie

Zielsetzung

Das Ziel dieser Richtlinie ist es, sicherzustellen, dass alle Informationen, die von der IT Manufactory GmbH und unseren Kunden über unsere Digital Automotive SaaS-Anwendung erhoben, gespeichert bzw. verarbeitet werden, zuverlässig, sicher und vollständig gesichert werden. Wir stellen sicher, dass alle gesicherten Daten vertraulich bleiben und dass wir alle geltenden Gesetze und Vorschriften einhalten.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter der IT Manufactory GmbH, wenn sie im Rahmen dienstlicher Tätigkeiten Datensicherungen einrichten, betreuen oder durchführen.

Verantwortlichkeiten

Die Verantwortung für die Datensicherung liegt bei IT Manufactory GmbH Security, Betrieb und unserem SaaS-Provider. Wir sind dafür verantwortlich sicherzustellen, dass die Daten regelmäßig gesichert und dass die Backups auf einem sicheren, verschlüsselten Speicherort aufbewahrt werden.

Datensicherung

Die IT Manufactory GmbH ist verantwortlich, dass alle Daten regelmäßig gesichert werden, um den Verlust von Daten durch unbeabsichtigtes Löschen, Hardware-Ausfälle, Sicherheitsvorfällen oder andere Ursachen zu minimieren. Wir führen regelmäßige Backups durch, um sicherzustellen, dass alle Daten geschützt sind und Verluste durch versehentliches Löschen, Hardwarefehler, Sicherheitsvorfälle oder andere Ursachen minimiert werden. Wir erstellen tägliche inkrementelle Backups sowie wöchentliche Vollbackups. Diese Backups werden auf Azure an einem verschlüsselten Speicherort mit bestimmten.

Zugangssteuerung

Die IT Manufactory GmbH steuert die Registrierung und Deregistrierung von Benutzern, dass ausschließlich eine Zuteilung von Benutzerzugängen einem berechtigten Personenkreis im Rahmen der Datensicherung erlaubt wird.

Wiederherstellung

Die IT Manufactory GmbH stellt im Falle eines Datenverlustes sicher, dass Informationen so schnell wie möglich wiederhergestellt und verfügbargemacht werden. Wir verwenden die Backups, um verlorene oder beschädigte Daten wiederherzustellen und sicherzustellen, dass alle Integrität und Verfügbarkeit wiederhergestellt. Ziel ist es, jeglichen Datenverlust zu vermeiden. Regelmäßige Datensicherungen und Wiederherstellungsmaßnahmen sollen dafür sorgen, dass im Falle eines Datenverlustes nur ein minimaler Datenverlust entsteht. Das genaue Ausmaß eines möglichen Datenverlustes hängt jedoch von verschiedenen Faktoren ab, wie z. B. der Häufigkeit der Datensicherungen und der seit der letzten Sicherung entstandenen Datenmenge. Es ist jedoch unser Bestreben, den potenziellen Datenverlust auf ein absolutes Minimum zu reduzieren. Im Falle eines Serverausfalls wird der maximale Datenverlust bis zum letzten Backup, das immer weniger als 24 Stunden zurückliegt, verhindert.

Kryptographischen Maßnahmen

Die IT Manufactory GmbH stellt sicher, dass alle gesicherten Informationen vertraulich bleiben.
Wir verwenden starke Verschlüsselungsprotokolle, um sicherzustellen, dass alle gesicherten Daten geschützt sind.

Überprüfung und Testen

Die IT Manufactory GmbH stellt sicher, dass alle Backups regelmäßig auf ihre Integrität und Vollständigkeit überprüft werden, um sicherzustellen, dass sie bei Bedarf wiederhergestellt werden können. Wir führen auch regelmäßige Tests durch, um sicherzustellen, dass unsere Backup- und Wiederherstellungsprozesse ordnungsgemäß funktionieren.

Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Die IT Manufactory GmbH hat die datenschutzrechtlichen Maßnahmen einschließlich Risikobetrachtung auch für Situationen, in denen Testdaten verwendet werden zu berücksichtigen.

Löschung von Daten

Die Backups werden automatisch gelöscht, sobald sie älter als 35 Tage sind. Wir achten auf die Einhaltung der üblichen Datenspeicherung und speichern die Daten nur so lange auf der Datenbank, wie es für den reibungslosen Betrieb erforderlich ist. Auf Wunsch ist es auch möglich, alle Benutzerdaten zu löschen. SaaS-Providers von Cloud-Speicher verwenden jedoch in der Regel Speichertechniken, um die physische Speicherkapazität effizient zu nutzen. Aufgrund dieser Techniken kann es einige Zeit dauern, bis die Daten vollständig gelöscht werden können.

Ereignisprotokollierung

Protokollierung von Backups und alle Arten von Datensicherungen werden soweit möglich zu jeder Zeit einsehbar. Protokoll-Informationen werden nur zu beauftragten Zwecken und dazu befugten Mitarbeitern der IT Manufactory GmbH genutzt. Alle Protokolle werden regelmäßig nach Ablauf von angemessenen und dokumentierten Fristen gelöscht.

Compliance

Die IT Manufactory GmbH stellt sicher, dass wir alle geltenden gesetzlichen Bestimmungen und vertragliche Anforderungen einhalten, die sich auf die Datensicherung beziehen.
Wir stellen sicher, dass alle gesicherten Informationen auf technische, sichere und rechtmäßige Weise behandelt werden.
Die Vorgehensweise der Organisation für die Handhabung der Datensicherung und deren Umsetzung werden auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft.
Dazu unterziehen wir unser ISMS einer regelmäßigen unabhängigen Prüfung durch externe Auditoren nach ISO 27001.

Änderungen

Die IT Manufactory GmbH behält sich das Recht vor, diese Datensicherungsrichtlinie jederzeit zu ändern. Wir informieren unsere Kunden über alle Änderungen und stellen sicher, dass sie auf dem Laufenden sind, was unsere Datensicherung betrifft.

Meldung bei Verstößen

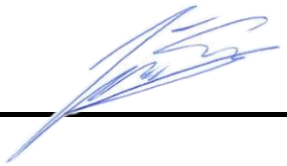
Vorgehensweise bei Verstößen gegen die Datensicherheitsrichtlinie.
Wenn personenbezogene Daten, Geschäftsgeheimnisse verletzt werden oder eine solche Verletzung droht (z.B. Verlust von Arbeitsgeräten oder Dokumenten, Hacker-Angriffen, Angriffen durch Schadsoftware etc.), hat der Mitarbeiter umgehend die Geschäftsführung, Vorgesetzten oder den Datenschutzbeauftragten zu informieren. Bei IT-Verstößen ist ferner unverzüglich die IT-Abteilung zu informieren.

Wichtige Kontaktdaten

IT-Notfälle: ISMS-Beauftragte siehe Notfall Kontakte

Ort, den

Passau, 14.03.2023



Geschäftsführung