Datensicherungsrichtlinie

Digital Automotive

Version: 1.2.0

Datum: 23.05.2025

Vertraulichkeit: gering

Verfügbarkeit: hoch

Integrität: hoch

Autor: Jürgen Sterr / CTO

Mitwirkende:

- Tobias Kellner / ISB

Interessierte Parteien:

- Mitarbeiter
- Kunden

Versionshistorie

Version	Datum	Geändert durch	Genehmigt von	Änderungen
1.0.0	18.07.2023	Jürgen Sterr	Erik Reiter	Dokument initial erstellt
1.1.0	07.01.2025	Tobias Kellner	Jürgen Sterr	Styling hinzugefügt, Aussagen konkretisiert
1.2.0	23.05.2025	Tobias Kellner	Jürgen Sterr	Datensicherung für Kubernetes Migration aktualisiert

1 Inhalt

2 Datensicherungsrichtlinie

2.1 Ziel

Diese Richtlinie verfolgt das Ziel, die Schutzziele der Informationssicherheit für alle Informationen zu gewährleisten, die von der IT Manufactory GmbH und unseren Kunden über die Digital Automotive SaaS-Anwendung gespeichert oder verarbeitet werden.
Alle gesicherten Daten werden vertraulich, unveränderbar und jederzeit verfügbar gehalten, wobei sämtliche geltenden Gesetze und Vorschriften eingehalten werden.

2.2 Geltungsbereich

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

2.3 Verantwortlichkeiten

Die Verantwortung für die Datensicherung liegt bei der DevSecOps-Abteilung der IT Manufactory GmbH und unseren Cloud-Service-Providern. Wir sind dafür verantwortlich, sicherzustellen, dass die Richtlinie zur Datensicherung regelmäßig überprüft und eingehalten wird. Zudem obliegt es uns, sicherzustellen, dass Daten regelmäßig gesichert und die Backups an einem sicheren, verschlüsselten Ort aufbewahrt werden.

2.4 Identifikation und Klassifizierung

Es muss eine Bestimmung erfolgen, welche Daten als offizielle Aufzeichnungen gelten und daher besonders geschützt werden müssen.
Diese Bestimmung erfolgt über die Einteilung der Aufzeichnungen in verschiedene Kategorien basierend auf ihrer Sensibilität und Wichtigkeit.
Weitere Informationen können der Klassifizierungsrichtlinie entnommen werden.

2.5 Datensicherung

IT Manufactory GmbH is responsible for ensuring that all data is regularly backed up to minimize the loss of data due to accidental deletion, hardware failures, security incidents, or other causes. Regular backups ensure that, in the event of an incident, data availability can be restored, and downtime is reduced.

2.5.1 Backup environments and systems

2.5.1.1 Production/Trial Systeme

Die Produktions- und Testsysteme werden über die Infrastruktur der Microsoft Azure Cloud bereitgestellt und sind an die Backup-Dienste von Azure angeschlossen, die zudem Verschlüsselung und Integritätsprüfungen auf die Backups anwenden. Sofern nicht anders angegeben, befindet sich der Hosting-Standort in *Nord Europe*. Es gelten die folgenden Backup-Richtlinien:

- **Datenbank:**
  Die Datenbanken werden über den Dienst „Azure Database for PostgreSQL – Flexible Server“ bereitgestellt. Tägliche automatische Vollsicherungen der Datenbanken werden durchgeführt. Die Backups werden 30 Tage lang aufbewahrt und georedundant gespeichert. Zusätzlich zur Cloud-Sicherung werden tägliche Vollsicherungen aller Datenbanken auf einem selbst gehosteten NAS-System erstellt. Diese täglichen Backups werden 30 Tage lang aufbewahrt, bevor sie automatisch gelöscht werden. Eine monatliche Sicherung vom 1. eines jeden Monats wird für mindestens 6 Monate aufbewahrt. Der Kunde kann eine vorzeitige Löschung der Daten beantragen (z. B. bei Beendigung der Geschäftsbeziehung). Dieses NAS-System ist mit RAID-Schutz ausgestattet, um zusätzliche Sicherheit gegen Hardware-Ausfälle zu gewährleisten. Die Backups sind ebenfalls verschlüsselt, um vor unbefugtem Zugriff zu schützen.
- **Dokumente & Bilder:**
  Die Dateiresourcen werden über den Dienst „Azure Storage Account – File Shares“ bereitgestellt. Es werden tägliche automatische Vollsicherungen des Dateispeichers durchgeführt. Diese täglichen Backups werden 30 Tage lang aufbewahrt. Eine monatliche Sicherung vom ersten Sonntag eines jeden Monats wird für 6 Monate gespeichert. Alle Backups werden georedundant gespeichert.
  Zusätzlich zur Cloud-Sicherung werden tägliche Vollsicherungen aller Dateiresourcen auf einem selbst gehosteten NAS-System erstellt. Diese täglichen Backups werden 30 Tage lang aufbewahrt, bevor sie automatisch gelöscht werden. Eine monatliche Sicherung vom 1. eines jeden Monats wird für mindestens 6 Monate aufbewahrt. Der Kunde kann eine vorzeitige Löschung der Daten beantragen (z. B. bei Beendigung der Geschäftsbeziehung). Dieses NAS-System ist mit RAID-Schutz ausgestattet, um zusätzliche Sicherheit gegen Hardware-Ausfälle zu gewährleisten. Die Backups sind ebenfalls verschlüsselt, um vor unbefugtem Zugriff zu schützen.

2.5.1.2 Staging Systeme

Die Staging-Systeme werden über die Infrastruktur von Digital Ocean bereitgestellt. Sofern nicht anders angegeben, befindet sich der Hosting-Standort in *FRA1*. Es gelten die folgenden Backup-Richtlinien:

- **Datenbank:**
  Es werden tägliche Vollsicherungen aller Datenbanken auf einem selbst gehosteten NAS-System durchgeführt. Diese täglichen Backups werden 30 Tage lang aufbewahrt, bevor sie automatisch gelöscht werden. Eine monatliche Sicherung vom 1. eines jeden Monats wird für mindestens 6 Monate aufbewahrt. Der Kunde kann eine vorzeitige Löschung der Daten beantragen (z. B. bei Beendigung der Geschäftsbeziehung). Dieses NAS-System ist mit RAID-Schutz ausgestattet, um zusätzliche Sicherheit gegen Hardware-Ausfälle zu gewährleisten. Die Backups sind ebenfalls verschlüsselt, um vor unbefugtem Zugriff zu schützen.
- **Dokumente & Bilder:**
  Es werden tägliche Vollsicherungen aller Dateiresourcen auf einem selbst gehosteten NAS-System durchgeführt. Diese täglichen Backups werden 30 Tage lang aufbewahrt, bevor sie automatisch gelöscht werden. Eine monatliche Sicherung vom 1. eines jeden Monats wird für mindestens 6 Monate aufbewahrt. Der Kunde kann eine vorzeitige Löschung der Daten beantragen (z. B. bei Beendigung der Geschäftsbeziehung). Dieses NAS-System ist mit RAID-Schutz ausgestattet, um zusätzliche Sicherheit gegen Hardware-Ausfälle zu gewährleisten. Die Backups sind ebenfalls verschlüsselt, um vor unbefugtem Zugriff zu schützen.

2.6 Zugangssteuerung

Die IT Manufactory GmbH steuert die Registrierung und Deregistrierung von Benutzern. Der Zugriff auf die Backup-Systeme und -Daten ist strikt reglementiert. Nur autorisierte Personen aus dem IT-Team der IT Manufactory GmbH erhalten Zugriff auf die Backup-Daten. Dieser Zugriff erfolgt auf Basis von Rollen und Rechten und wird regelmäßig überprüft und angepasst.

2.7 Physischer Schutz

Nutzung sicherer physischer Standorte zur Aufbewahrung von Aufzeichnungen, z.B. abschließbare Schränke, sichere Rechenzentren und gesicherten eigenen Serverräumen.
Einsatz von Überwachungssystemen wie Kameras, Alarmanlagen und Zugangskontrollsystemen, um physischen Zugang zu den Aufzeichnungen zu kontrollieren und zu überwachen.

2.8 Backup- und Wiederherstellungsverfahren

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. Die Integrität dieser Daten kann gewährleistet werden. Das Ziel ist, jeglichen Datenverlust zu verhindern. Regelmäßige Datensicherungen und Wiederherstellungsverfahren sind implementiert, um sicherzustellen, dass im Falle eines Datenverlusts nur ein minimaler Verlust auftritt. Das genaue Ausmaß eines möglichen Datenverlusts hängt jedoch von verschiedenen Faktoren ab, wie der Häufigkeit der Datensicherungen und der Menge der seit der letzten Sicherung erstellten Daten. Dennoch streben wir an, potenzielle Datenverluste auf ein absolutes Minimum zu reduzieren. Im Falle eines Ausfalls wird der maximale Datenverlust bis zur letzten Sicherung verhindert, die immer weniger als 24 Stunden zurückliegt.

2.9 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 und deren Vertraulichkeit gewährleistet ist.
Nähere Informationen können der Richtlinie zum Gebrauch von kryptographischen Maßnahmen entnommen werden.

2.10 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 regelmäßige Notfalltests durch, um sicherzustellen, dass unsere Backup- und Wiederherstellungsprozesse ordnungsgemäß funktionieren und die Wiederherstellungszeit auf ein Minimum reduziert werden kann.

2.11 Trennung Betriebsumgebungen

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

Weitere Informationen zur Trennung von Betriebsumgebungen können dem Kapitel A 12.1.4 entnommen werden.

2.12 Löschung von Daten

Die Aufbewahrungsfristen für Backups werden unter Berücksichtigung gesetzlicher und betrieblicher Anforderungen festgelegt. Die genauen Aufbewahrungsfristen sind bereits im Punkt **Datensicherung** genannt worden. Abgelaufene Backups werden nach festgelegten Löschrichtlinien sicher und vollständig gelöscht. Wir speichern Daten nur so lange, wie es für den reibungslosen Betrieb, vertragliche- oder für gesetzliche- Anforderungen erforderlich ist. Ein Beispiel für eine gesetzliche Anforderung ist die Datenschutz-Grundverordnung. So werden alle Daten des Kunden gelöscht, wenn z.B. das Geschäftsverhältnis beendet wird, da der Zweck der Datenverarbeitung entfällt. Zu beachten sind eventuelle Ausnahamen aufgrund anderer gesetzlicher Vorgaben. Die Löschung einzelner Datensätze (z.B. Benutzerdatensätze) ist auf Wunsch ebenfalls möglich. Die IT Manufactory GmbH verpflichtet sich, eine Datenlöschung innerhalb von einer Woche nach Bekanntwerden durchzuführen.

Außerdem ist zu erwähnen, dass unsere Cloud-Provider Speichertechniken einsetzen, die gewährleisten, dass die physische Speicherkapazität effizient genutzt wird. Daher kann die endgültige physische Löschung der Daten einige Zeit in Anspruch nehmen. Auf diesen Vorgang hat die IT Manufactory GmbH keinen Einfluss.

2.13 RTO & RPO

2.13.1 Recovery Time Objective

Das Recovery Time Objective (RTO) definiert die maximal zulässige Ausfallzeit für die Wiederherstellung von Diensten nach einer Unterbrechung, um die Auswirkungen auf den Betrieb so gering wie möglich zu halten. Für alle Dienste ist das RTO auf 4 Stunden festgelegt, wenn der Ausfall während der Arbeitszeiten bemerkt wird. Die Arbeitszeiten sind von Montag bis Freitag von 8:00 bis 17:00 Uhr MEZ/MESZ definiert (ausgenommen nationale Feiertage). Backupsysteme und Wiederherstellungsprozesse sind darauf ausgelegt, dieses Ziel zu erreichen, wobei regelmäßige Tests die Einhaltung überprüfen. Im Falle eines Vorfalls haben Wiederherstellungsmaßnahmen das vorrangige Ziel, die Verfügbarkeit der Dienste innerhalb des definierten RTO sicherzustellen, um die betriebliche Kontinuität zu wahren und das Risiko längerer Ausfälle zu minimieren.

2.13.2 Recovery Point Objective

Das Recovery Point Objective (RPO) legt den maximal zulässigen Datenverlust in zeitlicher Hinsicht während einer Unterbrechung fest und definiert den Zeitpunkt, auf den Daten wiederhergestellt werden müssen, um den Betrieb fortzusetzen. Für alle Dienste ist das RPO auf 24 Stunden festgelegt, wodurch sichergestellt wird, dass Backups häufig genug erstellt werden, um den betrieblichen Anforderungen gerecht zu werden. Backup-Zeitpläne und Replikationsprozesse sind so konfiguriert, dass sie mit diesem Ziel übereinstimmen und potenzielle Datenverluste minimieren. Regelmäßige Überprüfungen und Tests werden durchgeführt, um sicherzustellen, dass die Backup-Systeme das definierte RPO einhalten, und so die Datenintegrität und Zuverlässigkeit gewährleisten.

2.14 Sekundärsysteme

Alle Sekundärsysteme, einschließlich, aber nicht beschränkt auf den Authentifizierungsdienst und den Messaging-Dienst, unterliegen denselben Backup-Richtlinien und -Verfahren wie der Hauptdienst. Diese Dienste sind entscheidend für die Gesamtfunktionalität und Sicherheit des Systems und müssen eine konsistente Datenintegrität und Verfügbarkeit gewährleisten. Regelmäßige Backups von Konfigurationsdateien, Logs, Datenbanken und anderen kritischen Daten, die mit diesen Nebendiensten verbunden sind, werden gemäß dem gleichen Zeitplan und den gleichen Aufbewahrungsfristen wie beim Hauptdienst durchgeführt. Darüber hinaus werden Wiederherstellungsprozesse regelmäßig getestet, um eine nahtlose Wiederherstellung im Falle eines Ausfalls sicherzustellen und dabei die definierten Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) des Hauptdienstes einzuhalten.

2.15 Ereignisprotokollierung

Das Logging von Backups und allen Arten von Datensicherungen ist jederzeit, soweit möglich, einsehbar. Log-Informationen werden ausschließlich für autorisierte Zwecke und von autorisierten Mitarbeitern der IT Manufactory GmbH genutzt. Alle Logs werden regelmäßig nach Ablauf angemessener und dokumentierter Zeiträume gelöscht.

2.16 Compliance

Die IT Manufactory GmbH stellt sicher, dass wir alle geltenden gesetzlichen Vorschriften und vertraglichen Anforderungen im Zusammenhang mit der Datensicherung einhalten. Wir gewährleisten, dass alle gesicherten Informationen auf eine sichere und rechtmäßige Weise behandelt werden. Der Umgang der Organisation mit dem Datenschutz und dessen Umsetzung wird in regelmäßigen Abständen oder bei wesentlichen Änderungen unabhängig überprüft. Zu diesem Zweck unterziehen wir unser ISMS regelmäßigen unabhängigen Audits durch externe Prüfer gemäß ISO 27001.

2.17 Aktualisierung

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

2.18 Meldung bei Verstößen

Wenn personenbezogene Daten oder Geschäftsgeheimnisse verletzt werden oder eine solche Verletzung droht (z. B. Verlust von Arbeitsgeräten oder Dokumenten, Hackerangriffe usw.), muss der Mitarbeiter unverzüglich die Geschäftsleitung oder den Vorgesetzten informieren. Gegebenenfalls ist auch die IT-Abteilung umgehend zu benachrichtigen.

2.19 Wichtige Kontaktdaten

Die genannten Personen sind in der Notfallkontaktliste der ISMS-Dokumentation aufgeführt.

IT Manufactory GmbH
Brunngasse 4, 94032 Passau / Deutschland
Tel: +49 (0) 800 14 14 14 7
E-Mail: info@digital-automotive-supplier.com
Web: https://digital-automotive-supplier.com