tesma Data Security & Protection - DURCHDACHTER SCHUTZ IHRER DATEN

1. Allgemeine Informationen

- **Was ist *tesma*?**
  tesma ist das Asset-Management-System von CHG-MERIDIAN, entwickelt als unterstützendes System für Leasingaktivitäten mit CHG-MERIDIAN. Es bietet Kunden Transparenz und Kontrolle über ihre geleasten Assets und stellt Funktionen wie Kostenübersicht, Vertragsmanagement und Reporting bereit. *tesma* wird seit über 20 Jahren in diesem Konzept betrieben.

- **Ist *tesma* eine Cloud-Lösung?**

  tesma ist **keine** traditionelle SaaS-Lösung, sondern eher mit einem Versicherungsportal vergleichbar. So wie ein Versicherungsportal sicheren Zugriff auf Versicherungsdaten bietet, ermöglicht *tesma* einen sicheren Zugriff auf leasingbezogene Daten und Prozesse. Dieser Unterschied ist wichtig, da *tesma* speziell auf die Bedürfnisse von Leasingkunden zugeschnitten ist und keine allgemeine Unternehmenssoftware darstellt.

- **Wo befinden sich die Rechenzentren von tesma?**

  Die Rechenzentren von *tesma* befinden sich in Deutschland, in der Nähe von Frankfurt, in Tier-III-Rechenzentren, deren Housing von NTT bereitgestellt wird. Die Server, einschließlich aller Daten und Anwendungen, werden vollständig von CHG-MERIDIAN betrieben und verwaltet. Diese Rechenzentren sind nach ISO 27001 und ISAE SOC zertifiziert.

  Zusätzlich werden einige spezifische Module von *tesma*, wie die Business-Applikation *Support*, auf der Infrastruktur von ServiceNow gehostet, die sich ebenfalls in Deutschland befindet. Die Hosting-Umgebung von ServiceNow entspricht den Standards von ISO 27001 und SOC 2 und gewährleistet ein hohes Maß an Sicherheit und Compliance nach aktuellem Stand der Technik.

---

2. Zertifizierungen

- ISO 27001: Für IT-Prozesse, einschließlich *tesma*.
- ISO 27701: Privacy Information Management System (PIMS), das die Einhaltung von Datenschutzanforderungen sicherstellt.
- ISO 22301: Business Continuity Management System (BCMS).
- ISO 37301: Compliance Management System, das die Einhaltung regulatorischer und gesetzlicher Anforderungen, einschließlich der BaFin-Vorschriften (Bundesanstalt für Finanzdienstleistungsaufsicht), sicherstellt.

- **Erfüllt *tesma* die Anforderungen der DSGVO?**
  Ja, *tesma* erfüllt alle Anforderungen der DSGVO vollständig.

---

3. Datensicherheit

- **Wie werden Daten in *tesma* verschlüsselt?**
    - **Während der Übertragung:** Daten werden mit TLS 1.3 verschlüsselt.
    - **Im Ruhezustand:** Backups werden mit 256-Bit-AES-Verschlüsselung gesichert.
- **Welche Maßnahmen gibt es gegen Angriffe von Dritten?**
    - Jährliche Penetrationstests.
- **Wie wird der Zugriff auf Daten verwaltet?**
  tesma verwendet das Need-to-Know-Prinzip. Kundenadministratoren verwalten die Benutzerberechtigungen, und alle Änderungen werden protokolliert.

---

4. Verfügbarkeit und Backups

- **Welche Verfügbarkeitsgarantie bietet *tesma*?**
  tesma garantiert eine Verfügbarkeit von 98 % pro Quartal, ausgenommen geplante Wartungsarbeiten (8 Stunden, zweimal pro Quartal, mit vorheriger Ankündigung).
- **Wie werden Daten gesichert?**
    - **Tägliche Backups:** Aufbewahrungszeitraum von 31 Tagen.
    - **Monatliche Backups:** Aufbewahrungszeitraum von 12 Monaten.
    - **Jährliche Backups:** Aufbewahrungszeitraum von 10 Jahren.
- **Werden Wiederherstellungstests durchgeführt?**
  Ja, Wiederherstellungstests werden regelmäßig durchgeführt, um die Wiederherstellbarkeit der Backups sicherzustellen.

---

5. Protokollierung und Überwachung

- **Was wird in *tesma* protokolliert?**
    - Jeder Login.
    - Änderungen, die von Benutzern vorgenommen werden, sind innerhalb der Anwendung nachvollziehbar.
    - Protokolle werden auf einem dedizierten Log-Server gespeichert.
- **Gibt es eine Überwachung?**
  Ja, *tesma* verfügt über eine Anwendungsüberwachung und ein Protokollmanagement.

---

6. Benutzer-Authentifizierung

- **Welche Authentifizierungsmethoden werden unterstützt?**
    - **Option 1:** Lokale Benutzerkonten – Nutzung des Identity Providers von CHG-MERIDIAN: Ein Benutzer wird im IDP angelegt, setzt ein Passwort und kann sich mit diesem anmelden. Diese Methode unterliegt einer Passwort-Richtlinie und entspricht den neuesten Standards in Technologie und Sicherheit.

      Option 2: Integration mit den Identity Providern des Kunden (z. B. Microsoft Azure AD) für Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA).

  Unsere Empfehlung: Integrieren Sie *tesma* immer mit dem Identity Provider Ihres Unternehmens (Option 2), um die Sicherheitsstandards Ihrer Organisation einzuhalten und die volle Kontrolle über das Benutzer-Management zu behalten.

- **Unterstützt *tesma* Multi-Faktor-Authentifizierung (MFA)?**
  Ja, *tesma* unterstützt MFA über die Integration mit dem Identity Provider des Kunden (Option 2).

---

7. Datenaufbewahrung und -löschung

- **Wie lange werden Daten in *tesma* aufbewahrt?**
  In *tesma* verfolgen wir eine Strategie, die darauf abzielt, nur relevante und aktuelle finanzielle Vertragsdaten anzuzeigen. Aus diesem Grund sind Mietscheine und die darin enthaltenen Assets ein Jahr nach vollständigem Abschluss des Mietscheins nicht mehr sichtbar.

- **Wie erfolgt die Datenvernichtung?**
  Daten werden gemäß den Datenschutzbestimmungen durch sicheres Überschreiben oder physische Zerstörung der Datenträger vernichtet.

---

8. Einbindung Dritter

- **Sind Drittanbieter beteiligt?**
  tesma wird hauptsächlich intern von CHG-MERIDIAN verwaltet. Einige spezifische Module, wie *Support* und *Procurement*, nutzen jedoch die Infrastruktur von ServiceNow. Die Hosting-Umgebung von ServiceNow befindet sich in Deutschland und entspricht den Standards von ISO 27001 und SOC 2, was ein hohes Maß an Sicherheit und Compliance gewährleistet.

- **Gibt es Datenübertragungen in Drittländer?**
  Ja, aber alle Daten werden von CHG-MERIDIAN verarbeitet.

- **Zusätzliche Schutzmaßnahmen:**
  CHG-MERIDIAN stellt sicher, dass ServiceNow strenge Sicherheits- und Compliance-Standards einhält.

---

9. Business Continuity

- **Verfügt *tesma* über einen Business Continuity Plan (BCP)?**
  Ja, CHG-MERIDIAN verfügt über ein ISO 22301-zertifiziertes Business Continuity Management System (BCMS), das *tesma* einschließt.
- **Was ist das Recovery Time Objective (RTO) für *tesma*?**
  Im unwahrscheinlichen Fall eines Disasters ist *tesma* so konzipiert, dass es minimale Unterbrechungen für Kunden verursacht: **RTA / RTO : 24h / 72h**
- **Was ist das Recovery Point Objective (RPO) für *tesma*?**
  Im unwahrscheinlichen Fall eines Disasters stellt *tesma* sicher, dass die Datenintegrität auf höchstem Niveau erhalten bleibt: **RPA / RPO : 24h / 24h**

---

10. *tesma* API

- **Integration und Funktionalität:**
  tesma ist eine digitale Plattform, die auf einem **API-First-Ansatz** basiert, um Assets zu verwalten, die bei CHG-MERIDIAN geleast werden. Die *tesma* APIs basieren auf den REST-Prinzipien, was die Integration von *tesma* in alle Geschäftsprozesse und Anwendungen erleichtert. Umfassende Informationen, einschließlich detaillierter Dokumentation und Beispiele, finden Sie im tesma IntegrationHub. Zu den wichtigsten Funktionen gehören:
  - Abruf von Leasingdaten, Berichten und Asset-Informationen.
  - Schreiben oder Aktualisieren spezifischer Datenpunkte nach Bedarf.
  - Überwachung des Systemzustands & Betriebsstatus über dedizierte Endpunkte.
- **Sicherheit, Kommunikation und Sitzungsmanagement:**
  - Die *tesma* API gewährleistet eine sichere Kommunikation durch TLS 1.3, um Datenintegrität und Vertraulichkeit während der Übertragung sicherzustellen.
  - API-Tokens werden für die Authentifizierung verwendet und müssen über die *tesma*-Weboberfläche generiert werden. Tokens sind aus Sicherheitsgründen nur einmal während der Erstellung sichtbar.
  - API-Tokens können mit einem Ablaufdatum von bis zu zwei Jahren konfiguriert werden, was Flexibilität für langfristige Integrationen bietet.
  - Kunden können Tokens verwalten und bei Bedarf widerrufen, um die Kontrolle über den API-Zugriff zu behalten.
- **Überwachung und Protokollierung:**
  - Alle API-Interaktionen, einschließlich Datenabruf und -aktualisierungen, werden protokolliert, um Nachvollziehbarkeit und Verantwortlichkeit sicherzustellen.
  - Tracing**:** Jede API-Anfrage wird mit einer eindeutigen Trace-ID versehen. Im Falle einer Fehlermeldung wird die Trace-ID im Antworttext angegeben.
  - Ein Health-Check-Endpunkt (https://api.tesma.com/status) steht zur Verfügung, um den Betriebsstatus der API in Echtzeit zu überwachen.