tesma Data Security & Protection - THOUGHTFUL PROTECTION OF YOUR DATA

1. General Information

- **What is *tesma*?**
  tesma is CHG-MERIDIAN's Asset-Management-System, designed as a **supporting system for leasing activities** with CHG-MERIDIAN. It provides customers with transparency and control over their leased assets, offering functionalities such as cost tracking, contract management, and reporting. *tesma* has been operating in this concept for over 20 years.

- **Is *tesma* a cloud solution?**

  tesma is **not** a traditional SaaS solution but is better compared to an insurance portal. Just as an insurance portal provides secure access to insurance data, *tesma* offers secure access to leasing-related data and processes. This distinction is important, as *tesma* is tailored to meet the specific needs of leasing customers rather than being a general-purpose enterprise software.

- **Where are *tesma* data centers located?**
  tesma data centers are located in Germany, near Frankfurt, in Tier III data centers where the housing is provided by NTT. The servers, including all data and applications, are fully operated and managed by CHG-MERIDIAN. These data centers are ISO 27001 and ISAE SOC certified.

  Additionally, some specific modules of *tesma* like the Business Application *Support* are hosted on ServiceNow infrastructure, which is also located in Germany. ServiceNow's hosting environment complies with ISO 27001 and SOC 2 standards, ensuring a high level of security and compliance in line with the latest state-of-the-art technology.

2. Certifications

- ISO 27001: For IT processes, including *tesma*.
- ISO 27701: Privacy Information Management System (PIMS), ensuring compliance with data privacy requirements.
- ISO 22301: Business Continuity Management System (BCMS).
- ISO 37301: Compliance Management System, ensuring adherence to regulatory and legal requirements, including BaFin (German Federal Financial Supervisory Authority) regulations.

- **Does *tesma* comply with GDPR?**
  Yes, *tesma* fully complies with all GDPR requirements.

3. Data Security

- **How is data encrypted in *tesma*?**
    - **In Transit:** Data is encrypted using TLS 1.3.
    - **At Rest:** Data is secured with 256-bit AES encryption.
- **What measures are in place against third-party attacks?**
    - Annual penetration tests.
- **How is data access managed?**
  tesma uses a need-to-know principle. Customer-Administrators manage user permissions, and all changes are logged.

---

4. Availability and Backups

- **What is *tesma's* availability guarantee?**
  tesma guarantees 98% availability per quarter, excluding planned maintenance (8 hours, twice per quarter, with prior notice).
- **How is data backed up?**
    - **Daily Backups:** Retention period of 31 days.
    - **Monthly Backups:** Retention period of 12 months.
    - **Annual Backups:** Retention period of 10 years.
- **Are restore tests performed?**
  Yes, restore tests are conducted regularly to ensure backup recoverability.

---

5. Logging and Monitoring

- **What is logged in *tesma*?**
    - Every login
    - Changes made by users are traceable within the application.
    - Logs are stored on a dedicated log server.
- **Is monitoring in place?**
  Yes, application monitoring and log management is in place for *tesma*.

---

6. User Authentication

- **What authentication methods are supported?**
    - **Option 1:** Local user accounts - Using CHG-MERIDIAN's identity provider: We do create a user in our IDP. User sets a password and can login with this password. This method is subject to a password policy and adheres to the latest standards in technology and security.

      Option 2: Integration with customer identity providers (e.g., Microsoft Azure AD) for Single Sign-On (SSO) and Multi-Factor Authentication (MFA).

  Our **recommendation** is to always **integrate with your customer identity provider (Option 2)**, as this ensures alignment with **your organization's security standards** and allows you to maintain **full control over user management**.

- **Does *tesma* support Multi-Factor Authentication (MFA)?**
  Yes, *tesma* supports Multi-Factor Authentication (MFA) via integration with the customer's identity provider (Option 2).

---

7. Data Retention and Deletion

- **How long is data retained in *tesma*?**
  In *tesma*, we follow a strategy designed to display only relevant and up-to-date financial contract data. For this reason, lease schedules and their included assets are no longer visible one year after the lease schedule has been fully completed.

- **How is data destruction handled?**
  Data is destroyed in compliance with data protection regulations, using methods such as secure overwriting or physical destruction of data carriers.

---

8. Third-Party Involvement

- **Are third-party providers involved?**
  tesma is primarily managed in-house. Some specific modules like *Support* and *Procurement*, utilize ServiceNow infrastructure. ServiceNow's hosting environment is located in Germany and complies with ISO 27001 and SOC 2 standards, ensuring a high level of security and compliance.

- **Is there any third-country data transfer?**
  Yes, but all data is processed by CHG-MERIDIAN.

- **Additional safeguards are in place.**
  CHG-MERIDIAN ensures that ServiceNow adheres to strict security and compliance standards.

---

9. Business Continuity

- **Does *tesma* have a Business Continuity Plan (BCP)?**
  Yes, CHG-MERIDIAN has an ISO 22301-certified Business Continuity Management System (BCMS), which includes *tesma*.
- **What is the Recovery Time Objective (RTO) for *tesma*?**
  In the unlikely event of a disaster, *tesma* is designed to ensure minimal disruption to customers **RTA / RTO : 24h / 72h**
- **What is the Recovery Point Objective (RPO) for *tesma*?**
  In the unlikely event of a disaster, *tesma* ensures that data integrity is maintained to the highest possible standard: **RPA / RPO : 24h / 24h**

---

10. *tesma* API

- **Integration and Functionality:**
  tesma is a digital platform based on an **API-first approach** to manage assets leased from CHG-MERIDIAN. The *tesma* APIs are built using REST principles, making it easy to integrate *tesma* into all your business processes and applications. Comprehensive information, including detailed documentation and examples, can be found at the tesma IntegrationHub. Key functionalities include:
  - Retrieving leasing data, reports, and asset information.
  - Writing or updating specific data points as required.
  - Monitoring system health and operational status through dedicated endpoints.
- **Security, Communication and Session Management:**
  - The *tesma* API ensures secure communication using TLS 1.3, providing data integrity and confidentiality during data transmission.
  - API tokens are used for authentication and must be generated within the *tesma* web interface. Tokens are only visible once during creation for security purposes.
  - API tokens can be configured with an expiration date of up to two years, offering flexibility for long-term integrations.
  - Customers can manage and revoke tokens as needed to maintain control over API access.
- **Monitoring and Logging:**
  - All API interactions, including data retrieval and updates, are logged to ensure traceability and accountability.
  - Tracing**:** Each API request is assigned a unique trace identifier. In case of an error response, the TraceId is included in the response body.
  - A health check endpoint (https://api.tesma.com/status) is available to monitor the API's operational status in real time.