**Company X – Requirements & Governance Framework**

(Legal, Technical and Operational Compliance)

### **Version: 1.0**

### **Date:**

## **Table of Contents**

1. Introduction
2. Chapter 1 – Legal & GDPR Framework
3. Chapter 2 – Information Security
4. Chapter 3 – Technical Architecture & Infrastructure
5. Chapter 4 – Service Delivery & SLA
6. Chapter 5 – Financial & Commercial Terms
7. Chapter 6 – Organisation & Continuity
8. Chapter 7 – Operational & Legal Delineation
9. Definition List
10. Self-Assessment Questions

## **1. Introduction**

This document defines the legal, technical, and operational requirements for **Company X**, a European IT platform facilitating the connection between software and hardware through APIs, connectors, and cloud-based integration tools.

The framework ensures:

* Compliance with EU and German regulations (GDPR, BDSG, NIS2, Data Act).
* Transparency, data protection and consistent governance.
* Clear delineation of responsibilities between Company X and its customers.

The platform is hosted in a **German data centre**, serving customers primarily within the **European Economic Area (EEA)**.

## **2. Legal & GDPR Framework**

### **2.1 Roles and Responsibilities**

* **Company X** acts as a **data processor** under the GDPR when processing personal data on behalf of customers.
* The **Customer** is the **data controller**, determining the purposes and means of processing.
* For data related to user accounts, billing and analytics, Company X is the **data controller**.
* A formal **Data Processing Agreement (DPA)** is concluded with each customer in accordance with Article 28 of the GDPR.

### **2.2 Data Protection and Storage**

* All data is hosted in **Germany** under the jurisdiction of the **GDPR** and **BDSG**.
* Any data transfers outside the EEA must use **Standard Contractual Clauses (SCCs)**.
* A published **list of sub-processors** identifies all third parties involved in data processing.

### **2.3 Transparency and Accountability**

* Company X maintains a **Security & Compliance Overview**, describing data flows, hosting, and security measures.
* Data protection by design and by default is implemented at all stages of system development.

## **3. Information Security**

### **3.1 Governance**

* Company X operates an **Information Security Management System (ISMS)** aligned with **ISO 27001** or equivalent.
* A **Security Officer** oversees implementation and monitoring of all security controls.

### **3.2 Technical Controls**

* Data is encrypted **in transit** (TLS 1.2+) and **at rest**.
* Multi-factor authentication (MFA) is mandatory for administrative users.
* Regular **penetration tests** and **vulnerability scans** are performed.
* **Backups** are made daily and tested for recovery.
* Role-based access control (RBAC) applies to all system access.

### **3.3 Incident Management**

* A documented **Incident Response Plan** defines roles, escalation and timelines.
* Breaches are reported within **72 hours**, as required by the GDPR.
* Customers are notified promptly of any incident affecting their data.

## **4. Technical Architecture & Infrastructure**

### **4.1 Cloud Environment**

* The platform is hosted in a certified **German data centre** (EEA).
* Data is logically separated across customers (multi-tenant architecture).
* The platform supports containerisation (Docker/Kubernetes) and scalable APIs.

### **4.2 System Architecture**

* RESTful APIs are used, documented via **OpenAPI/Swagger**.
* A **sandbox environment** is provided for testing and safe experimentation.
* Continuous Integration / Continuous Deployment (CI/CD) processes ensure stability.

### **4.3 Logging & Monitoring**

* All operations are logged (audit trails).
* Customers can access usage and error logs through their dashboard.
* Log retention complies with data minimisation and privacy principles.

## **5. Service Delivery & SLA**

### **5.1 Service Levels**

* **Uptime guarantee:** minimum 99.9% monthly availability.
* **Maintenance windows:** announced at least 48 hours in advance.
* **Incident response times** defined by severity.
* **Service credits** apply if SLA targets are not met.

### **5.2 Contractual Terms**

* **Notice period:** minimum of one month before termination.
* **Data export:** customers can retrieve all data upon termination.
* Optional **escrow agreement** for source code or configuration.
* Any tariff change must be announced at least 30 days in advance.

## **6. Financial & Commercial Terms**

### **6.1 Cost Structure**

* **Fixed costs:** subscription fees (subject to annual indexation).
* **Variable costs:** based on actual use (API calls, data traffic, storage).
* All cost components must be transparent and itemised.

### **6.2 Indexation**

* Annual price adjustment based on the **Eurostat HICP (Euro Area)**.
* Minimum 0%, maximum 5% per year.
* Indexation applies only to fixed fees, not usage-based components.

### **6.3 Billing**

* Invoices are issued electronically (monthly or annually).
* Payment terms: 30 days from invoice date.

## **7. Organisation & Continuity**

### **7.1 Structure and Governance**

* Company X is a legal entity established within the European Union.
* An internal governance framework defines roles and accountability for compliance.

### **7.2 Business Continuity**

* A **Business Continuity Plan (BCP)** ensures service resilience.
* Backups are stored in a secondary EEA location.
* Data remains available for export at least 30 days after contract termination.

### **7.3 Compliance**

Company X complies with the following EU frameworks:

* **General Data Protection Regulation (GDPR)**
* **Bundesdatenschutzgesetz (BDSG)**
* **NIS2 Directive (EU) 2022/2555**
* **EU Data Act (EU 2023/2854)**
* **Digital Services Act (EU 2022/2065)**
* **AI Act (EU 2024/1689)** where applicable

## **8. Operational & Legal Delineation**

### **8.1 General Principle**

Company X provides a **digital bridge** between software and hardware.  
Its responsibility ends at the **data transfer boundary** within the platform.  
Customers remain responsible for the software, data integrity, and hardware implementation.

### **8.2 Responsibility Matrix**

| **Domain** | **Company X Responsible** | **Customer Responsible** |
| --- | --- | --- |
| Platform maintenance and security | (✅) | (❌) |
| Data processing within the platform | ✅ (Processor?) | ✅ (Controller?) |
| Accuracy and security of custom code |  |  |
| Hardware operation and safety |  |  |
| Data privacy compliance (application side) |  |  |
| API connectivity and uptime |  |  |
| Compliance with sector-specific laws (e.g. CE, MDR) |  |  |

### **8.3 Liability Boundaries**

* Company X bears responsibility for infrastructure security and service continuity.
* Customers bear responsibility for correct configuration and legal use of the generated integrations.
* Company X excludes liability for damages caused by:
  + Customer’s own code or configuration errors.
  + Hardware malfunction or non-compliance.
  + Sectoral or product-specific obligations.

## **Definition List**

(Summary of key definitions, extend as needed)

| **Term** | **Definition** |
| --- | --- |
| **Company X** | The entity that owns and operates the Platform. |
| **Customer** | The natural or legal person using the Platform. |
| **Platform** | The digital infrastructure and environment provided by Company X. |
| **Data Processing Agreement (DPA)** | Agreement under GDPR Art. 28 defining data processing terms. |
| **Datacentre (Germany)** | The physical facility where all platform data is hosted within the EU. |
| **SLA (Service Level Agreement)** | Agreement specifying uptime, response times, and service credits. |
| **Uptime / Downtime** | Periods of operational availability / unavailability. |
| **Indexation** | Annual adjustment of fixed fees according to Eurostat HICP. |
| **Incident** | An event that affects the confidentiality, integrity or availability of the service. |
| **Business Continuity Plan (BCP)** | Document describing service continuity in case of disruption. |

## **Self-Assessment Questions**

| **Question** | **Answer** | **Action** | **Responsible** | **Status** |
| --- | --- | --- | --- | --- |
| Have all roles (controller vs processor) been formally documented? |  |  |  |  |
| Is a valid DPA signed with each customer? |  |  |  |  |
| Are all sub-processors listed and reviewed annually? |  |  |  |  |
| Is data hosted exclusively in Germany / EEA? |  |  |  |  |
| Is the ISMS implemented and audited? |  |  |  |  |
| Are penetration tests performed regularly? |  |  |  |  |
| Are data breaches reported within 72 hours? |  |  |  |  |
| Are uptime metrics (××?%) met and recorded monthly? |  |  |  |  |
| Are fixed and variable costs clearly distinguished? |  |  |  |  |
| Is annual indexation applied according to Eurostat HICP? |  |  |  |  |
| Is a Business Continuity Plan in place and tested? |  |  |  |  |
| Is customer responsibility for hardware and code clearly stated? |  |  |  |  |
| Is liability limited appropriately in the contracts? |  |  |  |  |
| Are all definitions used consistently across ToS, SLA and DPA? |  |  |  |  |