

Projekt-ID: SDG-M1

Synthetic Data Generator (SDG) – Overview and System Architecture

Version: 2.0

Status: 100/100 Validiert

Executive Summary

The Synthetic Data Generator (SDG) is an optional framework module for MaxOneOpen, designed to generate high-quality, fully auditable synthetic training data. It operates independently but integrates seamlessly with MaxTune and MaxAudit. SDG enables the creation of autonomous, privacy-first training datasets, reinforcing system sovereignty without external dependencies.

Note: This document builds upon earlier conceptual drafts and formalizes the structured framework according to TBYD and MaxOne architectural standards.

Scope and Objective

The SDG framework provides synthetic data generation capabilities for MaxOneOpen-based systems. Its primary objectives are:

- Full independence from external datasets
- Continuous internal validation and adaptation
- Strict adherence to TBYD and MaxOne audit principles
- Edge-native, decentralized operation
- Compliance with UDUH and Zero-Knowledge standards

Technical Background

The SDG architecture is built following the MaxOne three-layer model (Solutions – Frameworks – Maschinenraum). All modules operate under Zero-Trust principles, support adaptive self-evolution, and guarantee that no persistent user-related data is generated or stored.

System Components

- Data Generation Engine
- Validation and Self-Assessment Engine
- Adversarial Simulation Module

- Security and Privacy Layer
- Update and Adaptation Management
- Governance and Audit Interface

Interfaces and Flows

The SDG interfaces directly with MaxTune for learning policy input, MaxAudit for validation event logging, and MaxReg for compliance checks. All data flows are fully documented and audit-ready.

Validation and Testing Criteria

All SDG-generated data batches undergo mandatory self-validation steps, including:

- Diversity testing
- Plausibility checks
- Bias detection
- Adversarial robustness tests

Compliance and Auditability

The SDG is designed to meet international compliance requirements, including:

- GDPR / DSGVO standards
- Post-Quantum Cryptography guidelines
- Zero-Trust security architecture
- Adaptive Evolution and Secure Update principles

All components are built to be fully auditable under ISO 27001, GDPR, and internal TBYD architectural standards.