

# Projekt-ID. SDG-M5

---

Synthetic Data Generator (SDG) – Adversarial Simulation and Noise Injection Module

Version: 2.0

Status: 100/100 Validiert

## Executive Summary

The Adversarial Simulation and Noise Injection Module enhances the robustness and resilience of synthetic datasets generated by the SDG. By systematically injecting controlled noise and adversarial patterns, it ensures that datasets can withstand perturbations, simulate real-world variances, and meet stringent adversarial testing criteria.

## Scope and Objective

This document outlines the design, functionality, and validation procedures for the Adversarial Simulation and Noise Injection Module. It supports quality assurance, stress testing, and compliance with security standards within the MaxOne and TBYD ecosystems.

## Technical Background

Adversarial resilience is critical for ensuring synthetic data remains effective under stress conditions. Noise injection simulates realistic data variance while adversarial simulation tests the system's ability to recognize, withstand, and recover from targeted distortions.

## Core Components

- Controlled Noise Generator: Introduces bounded random variations into synthetic datasets.
- Adversarial Pattern Generator: Simulates structured attacks (perturbations, consistency violations).
- Resilience Testing Engine: Measures impact on data plausibility and integrity.
- Recovery and Revalidation Logic: Triggers automatic regeneration if resilience thresholds are not met.

## Interfaces and Integration Points

Key integration points include:

- Validation and Self-Assessment Framework: Adversarial testing results are incorporated

into final validation.

- MaxAudit: Logging of noise injection and adversarial events for audit trails.
- MaxTune: Adjustment of learning policies based on adversarial stress test outcomes.

## **Validation and Testing Criteria**

Performance metrics include:

- Noise Diversity Thresholds
- Adversarial Resilience Ratings
- Recovery Effectiveness Scores
- Logging Completeness for Auditability

## **Compliance and Auditability**

All adversarial and noise processes are fully compliant with:

- GDPR / DSGVO standards (anonymized testing)
- ISO 27001 resilience frameworks
- TBYD 100/100 validation principles
- MaxOne Edge Execution Standards