SECURE GALVANO AI

Datensicherheit & Compliance

Verwendete Methoden und Standards

Herausgeber	Stefan Maier — secure galvano ai
Rolle	KI-Entwicklung Oberflächentechnik, Materialphysiker
Web	secure-galvano-ai.com
Kontakt	smaier@rvh.at

Stand: 02.07.2026

Compliance ist kein Selbstzweck. Wenn Hauptkunden auditieren oder eine Behörde nachfragt, müssen Galvanikbetriebe nachweisen können, dass auch ihre Software-Lieferanten sauber arbeiten. OEM-Kunden in der Automobilindustrie verlangen zunehmend Nachweise zur Datensicherheit ihrer Lieferanten; ab Oktober 2026 greift in Österreich das NISG (NIS-2-Umsetzung), in Deutschland und der Schweiz bestehen parallele Regelungen.

Dieses Statement fasst zusammen, welche regulatorischen Rahmenwerke und Sicherheitsstandards bei der KI-Diagnose und einem späteren Live-System adressiert werden — und wie das in der Praxis aussieht. Es ist so formuliert, dass es intern weitergegeben oder im Erstgespräch gemeinsam durchgegangen werden kann. Ein detaillierter Konformitäts-Bericht für die Compliance-Abteilung eines Hauptkunden oder als Anhang zu einer Förderung wird auf Anfrage zugesendet.

EU AI Act

Verordnung 2024/1689 · gültig schrittweise ab 2025/2026

Die EU teilt KI-Systeme in vier Risikoklassen ein. Die Anomalieerkennung ist als Advisory-System ausgelegt: Auffälligkeiten werden markiert, die Reaktion entscheidet immer eine geschulte Fachkraft. Damit fällt sie in „minimal/limited risk" — es ist keine Hochrisiko-Konformitätsbewertung erforderlich. Für jede markierte Anomalie ist nachvollziehbar, welche Sensoren und welche Datenmuster sie verursacht haben (Explainable AI). Es erfolgen keine automatischen Eingriffe in die Anlage.

NIS2 / NISG 2026

Richtlinie 2022/2555 · NISG-Umsetzung in Österreich ab 10/2026

NIS2 verpflichtet größere Industriebetriebe zu Cybersecurity-Risikoanalyse, Incident-Reporting und Lieferkettensicherheit. Kleinere Betriebe sind nicht direkt erfasst — aber NIS2-pflichtige Hauptkunden reichen die Anforderung an ihre Lieferanten weiter. Die Diagnose-Methodik ist so dokumentiert, dass sie als Nachweis gegenüber auditierenden Kunden taugt: Patch-Prozesse, Logging und das Vorgehen bei Sicherheitsvorfällen sind festgehalten.

EU Cybersecurity Act 2.0

Anwendbar seit 01/2026

Der Cybersecurity Act fokussiert auf sichere Entwicklungsprozesse und Lieferketten-Security. Jede Code-Änderung läuft durch sieben automatisierte Prüfungen (unter anderem statische Codeanalyse, Abhängigkeitsprüfung, Lizenz-Check). Commits werden kryptografisch mit einem Hardware-Token (Yubikey) signiert, Änderungen sind über die gesamte Historie nachvollziehbar. Kritische Sicherheitsupdates werden innerhalb weniger Tage ausgeliefert.

DSGVO

Verordnung 2016/679 · Art. 32 Datensicherheit

Verarbeitet werden ausschließlich Maschinendaten — Sensorwerte, Prozessparameter, Reklamationsstatistiken. Personenbezogene Daten kommen weder in die Auswertung noch in das Modell. Die Sicherheitsanforderungen aus Artikel 32 sind trotzdem umgesetzt: Verschlüsselung bei der Übertragung, Zugriffskontrolle, dokumentierte Löschung nach Projektende. Sollten Datenexporte versehentlich personenbezogene Daten enthalten (z. B. Bediener-Namen in Schichtprotokollen), werden diese vor der Analyse entfernt und das Vorgehen schriftlich festgehalten.

IEC 62443-2-1

Industrial Control Systems Security · Edition 2024

IEC 62443 ist der zentrale Standard für Cybersecurity in industriellen Steuerungssystemen. Ein wichtiges Prinzip ist der einseitige Datenfluss: Daten dürfen von der Anlage zur Auswertung fließen, niemals zurück. So kann auch ein kompromittiertes Auswertungssystem den Produktionsprozess nicht manipulieren. Diese Trennung ist in der Architektur fest verankert — die Auswertung läuft auf einem abgeschotteten lokalen System mit ausschließlich lesendem Zugriff. Keine Schreibrechte auf SPS, Bad-Steuerung oder Anlagentechnik. Das ist nicht nur technische Maßnahme, sondern auch vertragliche Zusage.

TÜV AUSTRIA Trusted AI

Inspection Framework · Modellprüfung abgeschlossen 06/2026

TÜV AUSTRIA bietet eine freiwillige Modellprüfung für KI-Systeme im industriellen Einsatz an. Geprüft werden unter anderem statistische Validierung, Reproduzierbarkeit, das Vorgehen bei Modell-Drift und die Trennung von Trainings- und Validierungsdaten. Die Inspektion erfolgte von Ende April bis Ende Mai 2026 auf Basis der eingereichten Dokumentation sowie eines Auditgesprächs mit Live-Demonstration des Modells und wurde im Juni 2026 abgeschlossen. Der Inspektionsbericht bestätigt, dass das System die erwarteten Anforderungen für seine Risikoklasse erfüllt und einen fortgeschrittenen Reifegrad in Entwicklung und Dokumentation aufweist.

Wie das im Alltag organisiert ist

Die internen Datensicherheits-Prozesse folgen den Prinzipien der ISO/IEC 27001 — Risikobetrachtung, Zugriffskontrolle, dokumentierte Verfahren, Vorfallreaktion. Die Entwicklung läuft auf einem getrennten Arbeitsgerät mit Festplattenverschlüsselung, Multi-Faktor-Authentifizierung und Hardware-Token für die Code-Signierung. Reale Kundendaten verbleiben ausschließlich auf dem lokalen System; für Entwicklungs-Tests kommen synthetische Daten aus einem digitalen Zwilling zum Einsatz.

Vor jedem Projektstart wird eine Geheimhaltungsvereinbarung unterzeichnet. Ihre Daten bleiben während des gesamten Projekts in einer geschützten Umgebung und werden auf Wunsch nach Projektende vollständig gelöscht, mit schriftlicher Bestätigung.

Kontakt

Für einen detaillierten Konformitäts-Bericht oder die Klärung eines konkreten Audit-Kontexts:

Stefan Maier · secure galvano ai · secure-galvano-ai.com · smaier@rvh.at · +43 681 8148 3538