Siegfried

Siegfried Artificial Intelligence Policy

Siegfried supports the responsible, ethical, secure and compliant use and development of Artificial Intelligence (AI) systems. AI may enhance productivity, quality and innovation, but it also creates risks relating to data privacy, cybersecurity, regulatory compliance, bias, transparency, intellectual property, integrity and patient safety. This Policy applies to all Siegfried entities, employees and, where relevant, third parties acting for or on behalf of Siegfried.

Compliance & Risk Management

All AI systems must comply with applicable internal and external requirements, including the Siegfried Personal Data Protection Regulations, the Siegfried Code of Conduct, internal information security guidelines, the EU AI Act, the GDPR, the Swiss FADP and applicable national data protection laws.

When used in GxP environments, AI will be used following the principles below in alignment with established GxP regulations (e.g. EU GMP Annex 11, FDA 21 CFR Part 11, ICH Q9/Q10) and emerging AI governance standards.

No AI system may be used, developed, tested, deployed or materially changed unless it has been assessed and approved through competent governance functions in accordance with internal procedures.

Prohibited AI practices under the EU AI Act are not permitted at Siegfried. This includes AI systems using manipulative or deceptive techniques, exploiting vulnerabilities, social scoring, unlawful emotion recognition in the workplace, unlawful biometric categorization, or unauthorised biometric surveillance or identification.

Data Privacy and Confidentiality

Personal data may be processed in or by AI systems only where the processing has a valid legal basis, is necessary and proportionate, transparent to the individuals concerned, and subject to appropriate technical and organisational safeguards. Where required, the relevant processing must be assessed, documented in the applicable privacy records and reviewed by the Data Privacy Office before go-live.

Confidential, strictly confidential, personal or sensitive personal data may only be processed in approved AI systems and in accordance with applicable data classification, access, retention and security requirements. Data used to train, test, validate or operate AI systems must be accurate, relevant, traceable and limited to what is necessary for the approved purpose.

Human Oversight and Accountability

AI systems must support, not replace, human accountability. Employees remain responsible for decisions, actions and outputs supported by AI. AI-generated outputs must be reviewed, validated and, where appropriate, edited or approved by a competent human before being used, relied upon or published.

AI systems used in critical, material or high-impact processes must include effective human oversight, including the ability to intervene, override, escalate, suspend or correct the AI output. AI must not make solely automated decisions producing legal or similarly significant effects on individuals unless expressly permitted by applicable law and approved through the required internal process.

Transparency, Explainability and Labelling

Siegfried aims to ensure that AI systems are transparent, understandable and auditable in proportion to their risk. Users and affected persons must receive appropriate information on AI use, system purpose, limitations, relevant data use and, where applicable, the logic and consequences of AI-supported decisions.

AI-generated content and outcomes of AI-driven decisions must be clearly labelled or disclosed where required by law, where there is a risk of misleading users or stakeholders, or where the content is published externally or used to inform the public.

Bias, Fairness and Model Quality

AI systems must be designed, implemented and monitored to reduce unfair, discriminatory or misleading outcomes, in line with applicable data protection and non-discrimination principles.

Training, validation, testing and operational datasets must be assessed, as appropriate, for quality, relevance, representativeness and potential bias.

Deployed AI systems must be reviewed at risk-based intervals for fairness, bias, accuracy, robustness, performance degradation and model drift. Where material issues are identified, corrective actions must be implemented, which may include retraining, recalibration, additional safeguards, restricted use or decommissioning.

Security and Robustness

AI systems must be protected against cybersecurity risks, including unauthorised access, data leakage, prompt injection, adversarial manipulation, model misuse and supply-chain vulnerabilities.

Appropriate measures include access controls, encryption, logging, monitoring, secure development practices, testing, incident management and resilience measures proportionate to the system's risk level.

Access to sensitive AI capabilities (including biometric identification, facial recognition, surveillance, or emotion recognition) must be strictly limited, risk-assessed and approved prior to use, and only where lawful, necessary and proportionate.

Governance, Boundaries and Redress

Each AI system must have clear ownership, defined responsibilities and documented boundaries, including intended use, limitations, prohibited use, accountability for outcomes and escalation paths. Model Owners, Data Owners, System Owners and other accountable functions must ensure lifecycle governance, documentation, monitoring and compliance.

Siegfried provides mechanisms to report, escalate, investigate and correct concerns relating to AI outputs, misuse, security incidents, bias, privacy issues or harmful outcomes. Where AI decisions or outputs affect individuals, appropriate mechanisms must be available to request human review, correction, objection or contestation in line with applicable data protection and internal procedures.

Culture & Awareness

Employees and relevant partners receive training and awareness on responsible AI use, data privacy, cybersecurity, bias, transparency, data integrity and ethical considerations. Siegfried's AI posture is to use AI in a controlled, human-centered and compliant manner that supports innovation while protecting individuals, company information, regulatory expectations and patient safety.

Siegfried Artificial Intelligence Policy
Edition 2026

Issued by
Siegfried Holding AG
Siegfried Information Security Board
Edition 2026

Contact
Siegfried Holding AG
Untere Brühlstrasse 4
4800 Zofingen, Switzerland
Phone +41 62 746 11 11
www.siegfried.ch