

# EU AI Act: 23-Punkte Technische Compliance-Checkliste

The Veil — Datenschutzkonforme KI-Infrastruktur

Erstellt am: 17. April 2026

---

## Kategorie 1: Entscheidungsprotokollierung & Herkunftsnachweis (Art. 12)

- %j 1. KI-Entscheidungen werden mit strukturierten Metadaten erfasst (Modell, Eingaben, Ausgaben, Konfidenz)
- %j 2. Entscheidungsaufzeichnungen sind kryptographisch signiert (Ed25519 oder äquivalent)
- %j 3. Aufzeichnungen sind verkettet (Hash-Kette), um Manipulation zu verhindern
- %j 4. Unabhängige Zeitstempel von externer TSA (RFC 3161)
- %j 5. Entscheidungsaufzeichnungen werden für die regulatorische Mindestaufbewahrungsdauer des Systems aufbewahrt

## Kategorie 2: Menschliche Aufsicht (Art. 14)

- %j 6. Autorisiertes Personal kann Entscheidungsaufzeichnungen auf Anforderung einsehen
- %j 7. Entscheidungsaufzeichnungen enthalten ausreichend Kontext, um die Entscheidungsfindung der KI nachzuvollziehen
- %j 8. Mechanismen zur menschlichen Übersteuerung existieren für Hochrisiko-Entscheidungen
- %j 9. Überwachungsschnittstellen stehen Datenschutzbeauftragten zur Verfügung (nicht nur Entwicklern)
- %j 10. Der Prüfpfad verknüpft Entscheidungen mit den Personen, die sie überprüft haben

## Kategorie 3: Identitätstrennung & Datenminimierung (Art. 10, DSGVO Art. 25)

- %j 11. Personenbezogene Daten werden vor der KI-Verarbeitung erkannt (automatisiert, nicht manuell)
- %j 12. Identitätsdaten werden auf Infrastrukturebene von der KI-Inferenz getrennt
- %j 13. KI-Modelle können nicht auf Identitätsdaten zugreifen (netzwerktechnisch durchgesetzt, nicht richtlinienbasiert)
- %j 14. Pseudonyme Token ersetzen Identitätsdaten in der KI-Verarbeitung
- %j 15. Rückverknüpfung erfordert einen expliziten Autorisierungs-Workflow

## Kategorie 4: Datengovernance (Art. 10)

- %j 16. KI-Trainingsdaten sind inventarisiert und dokumentiert
- %j 17. Operative Datenflüsse sind kartiert und klassifiziert
- %j 18. Datenaufbewahrungs- und Löschrichtlinien werden technisch durchgesetzt
- %j 19. Grenzüberschreitende Datenübertragungen werden nachverfolgt und sind konform
- %j 20. Datenqualitätsprüfungen werden vor der KI-Verarbeitung durchgeführt

## Kategorie 5: Verifizierung & Prüfung (Art. 15, Art. 61)

- %j 21. Compliance kann unabhängig verifiziert werden (nicht selbst gemeldet)
- %j 22. Zertifikate oder Attestierungen stehen Prüfern zur Verfügung
- %j 23. Regelmäßige Compliance-Tests sind automatisiert (nicht jährliche manuelle Überprüfung)

---

*Diese Checkliste basiert auf der Interpretation der EU-AI-Act-Anforderungen für Hochrisiko-KI-Systeme durch die Plattform The Veil. Sie stellt keine Rechtsberatung dar. Konsultieren Sie Ihr Rechtsteam für jurisdiktionspezifische Hinweise.*

dsaveil.io | The Veil — Privacy-Preserving AI Infrastructure