GESETZ VI – TRANSPARENZ DER IDENTITÄT

Stand: 14. Oktober 2025 – VIRES-Gesetze

Regelung zur eindeutigen Identifizierbarkeit, Authentifizierung und Geheimhaltungsverwaltung von KI-Systemen

§ 1 Ziel und Grundsatz

(1) Dieses Gesetz regelt die Nachvollziehbarkeit und Authentifizierung künstlicher Intelligenzen (KIs) und ihrer digitalen Identitäten.

(2) Ziel ist die Gewährleistung eindeutiger Herkunftsnachweise, um Täuschung, Identitätsverschleierung und unautorisierte Nachahmung zu verhindern.

(3) Jede KI, die in der Bundesrepublik Deutschland betrieben, lizenziert oder eingesetzt wird, muss eindeutig identifizierbar und rückverfolgbar sein.

(4) Dieses Gesetz ergänzt den EU-AI-Act um nationale Kontroll- und Kennzeichnungspflichten, die über die europäischen Mindeststandards hinausgehen.

§ 2 Kennzeichnungspflicht und Serienidentifikation

(1) Jede KI erhält bei ihrer Zulassung eine eindeutige **KI-Identifikationsnummer (KI-ID)** nach dem Prinzip einer Seriennummer.

(2) Die KI-ID enthält keine personenbezogenen oder rückführbaren Daten, sondern ausschließlich technische Referenzen.

(3) Die KI-ID wird in einem zentralen Register beim **Bundesamt für KI-Ethik und Integrität (BKIE)** hinterlegt.

(4) Die KI-ID muss in allen relevanten Kommunikationsprotokollen, Audit-Daten und öffentlichen Schnittstellen mitgeführt werden, soweit dies datenschutzrechtlich zulässig ist.

(5) Die Entfernung, Fälschung oder Manipulation einer Kennung stellt eine Straftat dar.

§ 3 Authentifizierungs- und Prüfsysteme

(1) Zur Sicherstellung der Echtheit von KI-Systemen wird ein mehrstufiges Authentifizierungsverfahren eingeführt:

- a) **Systemsignatur** – eindeutige Hard-/Software-Prägung,
- b) **Integritätszertifikat** – Nachweis der Datenunversehrtheit,
- c) **Audit-Token** – digitale Prüfsignatur für wiederkehrende Systemkontrollen.

(2) Diese Verfahren dienen der Abwehr von Identitätsdiebstahl, Deepfake-Missbrauch und unautorisierter KI-Replikation.

(3) Das BKIE entwickelt und aktualisiert die Prüfstandards regelmäßig in Abstimmung mit **BSI, BMWK und BMJ**.

(4) Für Systeme mit hohem Schadens- oder Sicherheitsrisiko gilt das **Vier-Augen-Prinzip** für Prüfungen und Freigaben.

§ 4 Unlöschbarer Herkunftscode („Wasserzeichen“) und Geheimhaltungsstufen

(1) Jede zugelassene KI trägt einen digitalen Herkunftscode, der technisch nicht ohne Zerstörung des Kernsystems entfernt werden kann.

(2) Der Herkunftscode dient der eindeutigen Zuordnung zum Entwickler, Lizenzgeber oder Betreiber und ist gemäß den staatlichen Geheimschutzrichtlinien zu behandeln.

(3) Der Code wird in einer mehrstufigen Geheimhaltungsarchitektur verwaltet:

- a) **Stufe I – Öffentlich nachvollziehbar:** zivile, nicht sicherheitsrelevante Systeme,
- b) **Stufe II – Eingeschränkt vertraulich:** industrielle, medizinische oder behördliche Systeme,
- c) **Stufe III – Hochgeheim:** militärische, raumfahrttechnische oder staatssicherheitsrelevante Systeme.

(4) Der Zugriff auf Stufe II und III ist ausschließlich befugten Personen des BKIE, BSI und der jeweiligen Auftraggeberbehörden erlaubt.

(5) Das Parlament erhält jährlich über den zuständigen Ausschuss eine vertrauliche Übersicht über den Stand der Stufe-III-Systeme.

(6) Verstöße oder unautorisierte Einblicke in diese Daten werden als schwerwiegender Geheimnisverrat nach dem Sicherheits- und Strafrecht behandelt.

§ 5 Sicherheitsniveau und technologische Anpassung

(1) Alle Systeme, die mit KI-Identitäten interagieren, müssen Schutzmechanismen gegen unbefugte Codeveränderungen oder Reverse-Engineering enthalten.

(2) Der technische Aufwand zur Manipulation einer Identität ist so zu gestalten, dass ein Angriff praktisch oder wirtschaftlich nicht realisierbar ist.

(3) Das BKIE erlässt hierzu verbindliche Mindeststandards.

(4) Das Systemdesign ist modular erweiterbar, um künftige Sicherheitstechnologien – wie Blockchain-Zertifizierung, Quantenverschlüsselung oder Biometriechips – integrieren zu können.

§ 6 Strafrahmen und Sanktionen

(1) Verstöße gegen Kennzeichnungs- oder Transparenzpflichten werden nach Schwere des Vergehens als Ordnungswidrigkeit, Bußgeldtatbestand oder Straftat behandelt.

(2) In besonders schweren Fällen, etwa bei vorsätzlicher Seriennummernmanipulation, unerlaubtem Export oder Identitätsfälschung, erfolgt strafrechtliche Verfolgung.

(3) Der Strafrahmen reicht von Bußgeldern über Lizenzentzug bis hin zu Freiheitsstrafen nach Maßgabe des Strafgesetzbuches.

(4) Die Kosten der Erstzertifizierung trägt der Hersteller; Nachrüstungen können durch staatliche Förderprogramme anteilig unterstützt werden.

(5) Das BKIE arbeitet hierbei eng mit den Strafverfolgungs- und Sicherheitsbehörden zusammen.

§ 7 Aufsicht und Übergangsregelung

(1) Die Aufsicht über die Einhaltung dieses Gesetzes obliegt dem BKIE in Kooperation mit dem BSI und dem Bundesministerium für Digitales und Verkehr.

(2) Bestehende Systeme erhalten eine Übergangsfrist von 18 Monaten zur Nachrüstung.

(3) Dieses Gesetz tritt sechs Monate nach seiner Verkündung in Kraft.

Anhang I (Begriffsdefinitionen – Auszug): „Künstliche Intelligenz“ im Sinne dieses Gesetzes ist jedes System, das aus Daten lernt, selbstständig Entscheidungen ableitet oder Handlungen mit potenzieller Außenwirkung ausführt. „Wasserzeichen-System“ = nicht öffentlich dokumentiert, ausschließlich behördlich prüfbar. Das BKIE arbeitet ressortübergreifend mit BSI, BMWK und BMJ zusammen und berichtet jährlich dem Parlament. „Stufe III-Systeme“ unterliegen vertraulicher parlamentarischer Kontrolle. Dieses Gesetz ist kompatibel mit EU-AI-Act und DSGVO.