VIRES-Gesetz V – „Verhältnismäßigkeit“ (Final v1)

Gesetz zur Sicherstellung angemessener, erforderlicher und zumutbarer Maßnahmen gegenüber KI-Systemen; mit risikobasierten Fristen, richterlicher Kontrolle bei Gefahr im Verzug, Beweissicherungspflichten und umsatzbezogenen Sanktionsrahmen.

§ 1 – Zweck, Geltungsbereich, Verhältnismäßigkeitsprinzip

(1) Dieses Gesetz konkretisiert die Anforderungen an die Verhältnismäßigkeit bei Entwicklung, Betrieb, Prüfung, Eingriffen, Sanktionen und Exporten von KI-Systemen der Stufen 1–5.

(2) Verhältnismäßigkeit im Sinne dieses Gesetzes umfasst drei Prüfungsschritte: **(a) Eignung** (die Maßnahme fördert den legitimen Zweck), **(b) Erforderlichkeit** (kein milderes, gleich wirksames Mittel verfügbar) und **(c) Angemessenheit** (der Eingriff steht nicht außer Verhältnis zum angestrebten Nutzen).

(3) Maßnahmen sind zeitlich, sachlich und organisatorisch auf das erforderliche Maß zu begrenzen und frühestmöglich zu beenden.

§ 2 – Stufenmodell der Eingriffe

(1) Eingriffe erfolgen grundsätzlich gestuft:

- Stufe 1 – *Information & Kooperation* (Auskunft, freiwillige Abhilfe),
- Stufe 2 – *Technische Sicherung* (Konfiguration einfrieren, Monitoring hochfahren, Quarantäne),
- Stufe 3 – *Operative Beschränkung* (Throttling/Rate-Limits, Rechteentzug, Sandbox-Betrieb),
- Stufe 4 – *Betriebsuntersagung/Abschaltung* (letztes Mittel),
- Stufe 5 – *Lizenzentzug/Exportstopp* (bei schweren oder wiederholten Verstößen).

(2) Das Überspringen von Stufen ist nur zulässig bei Gefahr im Verzug oder wenn mildere Mittel offensichtlich unzureichend sind; die Entscheidung ist zu begründen und zu protokollieren.

§ 3 – Erforderlichkeit und mildeste Mittel

(1) Vor Anordnung eingriffsintensiver Maßnahmen sind mildere, gleich wirksame Mittel vorzuziehen, insbesondere: Throttling/Rate-Limiting, isolierte Sandbox/Quarantäne, temporäre Rechtebeschränkung, Hotfix/Re-Training, erhöhtes Monitoring mit Human-in-the-Loop.

(2) Erweist sich ein milderes Mittel als unzureichend oder untauglich, können weitergehende Maßnahmen angeordnet werden.

§ 4 – Gefahr im Verzug, richterliche Kontrolle und Eingriffsfolgenabschätzung

(1) Bei akuter erheblicher Gefahr für Leben, Gesundheit, öffentliche Sicherheit oder massiven volkswirtschaftlichen Schaden dürfen Maßnahmen der Stufen 2–4 sofort angeordnet werden.

(2) Eine im Sinne des Absatzes 1 getroffene Maßnahme ist **binnen 72 Stunden** dem zuständigen Gericht zur nachträglichen Bestätigung vorzulegen; erfolgt keine Bestätigung, endet die Maßnahme mit Fristablauf.

(3) Unabhängig davon ist **binnen 7 Tagen** eine formelle Eingriffsfolgenabschätzung nachzureichen.

§ 5 – Datenzugriffe und Datenschutzgrundsätze

(1) Datenzugriffe (Logs, Modelle, Trainingsdaten, Konfigurationen) erfolgen zweckgebunden und nach dem Grundsatz der Datenminimierung; es gelten die Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität/Vertraulichkeit, Rechenschaft).

(2) Schutzstufen nach Ampelprinzip (Grün/Gelb/Rot) sind zu beachten; Einsicht in Rot-Daten setzt Splitschlüssel-Freigabe und zwingende Notwendigkeit voraus. Näheres regelt der Anhang A.

§ 6 – Eingriffsfolgenabschätzung und Mehr-Augen-Prinzip

(1) Vor Erlass eingriffsintensiver Maßnahmen ist eine Eingriffsfolgenabschätzung zu erstellen; sie wird Bestandteil der Verfahrensakte.

(2) Für Maßnahmen der Stufen 4 und 5 gilt ein Mehr-Augen-Prinzip: Entscheidungen sind von mindestens zwei unabhängigen Prüfern zu bestätigen (mindestens ein juristisch, ein technisch qualifizierter Prüfer). Bei umfangreichen oder sicherheitsrelevanten Eingriffen ist ein Vier- bis Sechs-Augen-Prinzip anzuwenden. Geringfügige Routinefälle (Stufen 1–3 ohne Risikoerhöhung) können unter Aufsicht nach Ein- bis Zwei-Augen-Prinzip entschieden werden. Schwellenwerte legt das BKIE per Verordnung fest.

§ 7 – Nachbesserungsfristen (risikobasiert)

(1) Nach Feststellung eines Defizits hat der Betreiber Nachbesserungen innerhalb der folgenden Fristen umzusetzen:

Risikokategorie	Definition (Beispiele)	Frist
Low	nicht sicherheitsrelevante Mängel, kosmetisch/funktional	90 Tage
Medium	funktionale Fehler ohne unmittelbare Gefährdung	30 Tage
High	erhebliche Gefährdung von Eigentum/Gesundheit	7 Tage
Critical	akute Gefahr im Verzug	Sofortmaßnahmen; Umsetzung binnen 48 Stunden

(2) Die Einstufung erfolgt durch die zuständige Behörde und ist zu begründen; Fristen können in begründeten Fällen verkürzt oder verlängert werden.

§ 8 – Dokumentation, Beweissicherung und Aufbewahrung

(1) Entscheidungen sind zu dokumentieren (Rechtsgrundlage, Zweck, Stufe, Dauer, Alternativen, Beendigungsstrategie).

(2) Vor Abschaltung oder tiefgreifenden Eingriffen ist ein vollständiger **Evo-Log-Snapshot** mit Signatur (WORM) zu erstellen und beim BKIE zu hinterlegen.

(3) Aufbewahrung: Unterlagen, Protokolle, Auditberichte werden nach Maßgabe des § 147 AO **mindestens zehn Jahre** revisionssicher aufbewahrt; für Systeme mit hoher gesellschaftlicher/sicherheitsrelevanter Tragweite kann die Frist per Verordnung auf **bis zu 40 Jahre** festgesetzt werden.

§ 9 – Rechte der Betroffenen und Rechtsbehelfe

(1) Betroffene haben Anspruch auf Anhörung, Akteneinsicht (soweit zulässig) und effektive Rechtsbehelfe.

(2) Bei Notfallmaßnahmen ist unverzüglich eine nachträgliche Anhörung sicherzustellen.

§ 10 – Entschädigung und Haftung

(1) Verursacht ein KI-System einen Schaden, haftet der jeweils Verantwortliche: bei Produkt-/Designmängeln der Hersteller, bei Betriebs-/Wartungsmängeln der Betreiber, bei unzulässigen Modifikationen der Integrator/Modifier.

(2) Ist eine eindeutige Zuordnung nicht möglich, haften Hersteller, Betreiber und Integratoren gesamtschuldnerisch; interner Regress bleibt unbenommen.

(3) Betreiber von Systemen der Stufen 3–5 haben eine Haftpflichtversicherung mit angemessener Mindestdeckung nachzuweisen; Näheres regelt eine Verordnung.

(4) Zur Sicherstellung schneller Entschädigungen kann ein nationaler KI-Regressfonds eingerichtet werden; Auszahlungen unterliegen strengen Prüf- und Rückforderungsregeln.

§ 11 – Sanktionen und technische Maßnahmen

(1) Ordnungswidrigkeiten werden gestaffelt geahndet:

- bis 1 Mio. EUR für Kleinst-/Kleinunternehmen,
- bis 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (je nachdem, was höher ist) für mittlere Unternehmen,
- bis 100 Mio. EUR oder 10 % des weltweiten Jahresumsatzes (je nachdem, was höher ist) für große Unternehmen.

(2) Bei vorsätzlicher, systematischer oder wiederholter Missachtung können zusätzlich die Betriebserlaubnis entzogen, Exportstopps verhängt sowie technische Maßnahmen (Blacklisting, dauerhafte Deaktivierung des betroffenen Systems) angeordnet werden.

(3) Die Anordnung der **permanenten Deaktivierung** bedarf einer besonderen Begründung und ist vor Vollziehung dem zuständigen Verwaltungsgericht zur Prüfung vorzulegen.

§ 12 – Internationale Zusammenarbeit

(1) Internationale Meldungen und Kooperationen erfolgen über die zuständigen EU-Koordinationsstellen (u. a. EU AI Office) sowie über Europol/Interpol und einschlägige bilaterale/multilaterale Abkommen.

(2) Standardisierte Forensik-Exporte und Datenformate sind zu verwenden; Datenschutz und Geheimschutz sind zu wahren. Näheres regelt der Anhang A.

§ 13 – Evaluierung und Inkrafttreten

(1) Dieses Gesetz ist **alle zwei Jahre** durch die zuständige Bundesbehörde zu evaluieren; Ergebnisse sind dem Deutschen Bundestag vorzulegen und bei Bedarf durch Verordnung umzusetzen.

(2) Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

(3) Ergänzende Definitionen, Schutzstufen und operative Leitlinien werden im **Anhang A (Begriffe & Prüfhinweise)** bereitgestellt.

Kurzbegründung: Der Entwurf verankert klassische Verhältnismäßigkeit (Eignung, Erforderlichkeit, Angemessenheit) in der KI-Praxis: gestufte Eingriffe, richterliche Kontrolle bei Gefahr im Verzug, risikobasierte Nachbesserungsfristen, Beweissicherung über Evo-Logs, starke aber verhältnismäßige Sanktionen (inkl. umsatzbezogener Bußgelder) sowie EU-konforme Kooperation.