# Gesetz zur Wahrung der digitalen Freiheit und des Datenschutzes („Digitales Freiheitsgesetz“)

**Präambel:**
In Anerkennung der grundlegenden Rechte auf Freiheit, Privatsphäre und informationelle Selbstbestimmung wird dieses Gesetz erlassen, um die Bürger vor jeglicher Form digitaler Überwachung, unkontrollierter Datensammlung und Missbrauch ihrer persönlichen Informationen zu schützen. Dieses Gesetz stellt sicher, dass keine zentrale Kontrolle über personenbezogene Daten entsteht und dass der Einzelne jederzeit die Hoheit über seine eigenen Informationen behält.

**§1. Grundsatz der digitalen Selbstbestimmung**

(1) Jeder Mensch hat das unveräußerliche Recht, über seine digitalen Daten zu bestimmen.
(2) Kein Staat, keine Behörde oder private Institution darf ohne ausdrückliche, freiwillige und informierte Zustimmung auf personenbezogene Daten zugreifen, es sei denn, es besteht eine unmittelbare, individuell begründete gesetzliche Notwendigkeit zur Verbrechensverfolgung.
(3) Eine Aggregation oder Vernetzung verschiedener persönlicher Datenquellen ist grundsätzlich untersagt.

**§2. Verbot der zentralisierten Datenspeicherung und Aggregation**

(1) Sämtliche digitale Identitäten, Gesundheitsdaten, Finanzinformationen und sonstige personenbezogene Daten dürfen ausschließlich dezentral gespeichert werden.
(2) Es ist untersagt, zentrale Datenbanken zu erstellen, die individuelle Datensätze verschiedener Lebensbereiche zusammenführen.
(3) Jeder Bürger hat das Recht, sämtliche über ihn gespeicherten Daten einzusehen und deren vollständige Löschung zu verlangen.

**§3. Zugangsbeschränkung und Zustimmungspflicht**

(1) Der Zugriff auf personenbezogene Daten darf nur nach individueller, temporärer Zustimmung des Betroffenen erfolgen.
(2) Jede Anfrage auf Datenzugriff muss durch eine ausdrückliche Genehmigung des Betroffenen bestätigt werden, die jederzeit widerrufen werden kann.
(3) Institutionen, Behörden und Unternehmen müssen ihre Datenanfragen detailliert begründen.
(4) Der Zugriff ist nur auf den spezifischen Datenbereich erlaubt, der für die jeweilige Interaktion notwendig ist (z. B. Gesundheitsdaten nur für Ärzte, Finanzdaten nur für Banktransaktionen).

**§4. Strenge Haftung und Sanktionen für Missbrauch**

(1) Jede missbräuchliche Verwendung, unautorisierte Speicherung oder Verknüpfung persönlicher Daten ist eine Straftat und wird mit der höchsten vorgesehenen Strafmaßnahme geahndet.
(2) Für Unternehmen, Behörden und Organisationen, die gegen dieses Gesetz verstoßen, gilt:
a) Erste Verstöße: Sofortige Löschung der erhobenen Daten, Bußgelder in Höhe von mindestens 10 % des Jahresumsatzes.
b) Wiederholte Verstöße: Ausschluss von öffentlichen Aufträgen, Lizenzentzug und strafrechtliche Verfolgung der verantwortlichen Führungskräfte.
c) Schwerwiegender Missbrauch (z. B. Verkauf oder unerlaubte Weitergabe personenbezogener Daten): Haftstrafen von bis zu 20 Jahren und existenzvernichtende Strafzahlungen.

**§5. Schutz vor übergriffigen Technologien (u. a. DigitalID, CBDC, Social Scoring bzw. Social-Credit-System)**

(1) Der Einsatz von Technologien zur digitalen Identifikation (DigitalID) ist nur zulässig, wenn eine anonyme Nutzung alternativer Zugangswege gewährleistet bleibt.
(2) Der digitale Euro (CBDC) oder ähnliche staatliche digitale Währungen dürfen nicht an individuelle Bürgerprofile gekoppelt werden, um soziale, wirtschaftliche oder politische Entscheidungen zu beeinflussen.
(3) Die Einführung jeglicher Form von Social Scoring oder KI-gesteuerter Bürgerbewertung ist

verboten.
(4) Die Verwendung von KI zur automatisierten Entscheidungsfindung über Bürgerrechte (z. B. Kreditvergaben, Reiseerlaubnisse, Zugang zu öffentlichen Dienstleistungen) ist unzulässig.

**§6. Transparenzpflicht und Bürgerkontrolle**

(1) Jede Instanz, die personenbezogene Daten erhebt oder verarbeitet, ist verpflichtet, vollständige Transparenz über die Art, Dauer und den Zweck der Datennutzung zu gewährleisten.
(2) Bürger haben das Recht auf eine vollständige Überwachung des Datenzugriffs in Echtzeit und müssen jeder Abfrage einzeln zustimmen können.
(3) Eine unabhängige Bürgerkontrollstelle wird eingerichtet, um Datenschutzverletzungen aufzudecken und Verstöße konsequent zu ahnden.

**§7. Abschaffung der verpflichtenden digitalen Identitäten**

(1) Die Nutzung digitaler Identitäten darf niemals verpflichtend sein.
(2) Jeder Bürger hat das Recht auf analoge Alternativen, insbesondere im Gesundheits-, Finanz- und Verwaltungswesen.
(3) Die Kopplung von DigitalID mit finanziellen, gesundheitlichen oder sozialen Dienstleistungen ist untersagt.

**§8. Schutz vor biometrischer Überwachung und KI-Überwachung**

(1) Der flächendeckende Einsatz von biometrischer Gesichtserkennung, KI-gestützter Massenüberwachung und Bewegungsprofilen ist verboten.
(2) Der Einsatz von KI zur Verhaltensanalyse und Überwachung öffentlicher Räume ist unzulässig.

**Schlussbestimmungen**

(1) Dieses Gesetz tritt sofort in Kraft.
(2) Jegliche bestehenden oder geplanten Gesetze, die diesem Gesetz widersprechen, sind unwirksam.
(3) Bürger können Verstöße direkt anzeigen und müssen dabei rechtlichen Schutz genießen.