

Universal Declaration on Digital Sovereignty and Data Rights (UDDSDR)

Marie Seshat Landry
Marie Landry's Spy Shop
www.marielandryceo.com

February 27, 2025

Adopted on February 27, 2025

Abstract

This Universal Declaration establishes fundamental principles regarding digital sovereignty, data privacy, and the ethical governance of personal and collective digital information. It affirms that individuals have the right to control their digital identities, data, and online presence, while governments and corporations must uphold transparency, security, and accountability in digital practices.

Contents

1	Definitions	2
2	General Principles	2
2.1	Right to Digital Ownership	2
2.2	Data Privacy and Consent	2
2.3	Protection from Algorithmic Discrimination	3
2.4	Right to Encryption and Security	3
2.5	Freedom from Mass Surveillance	3
3	Ethical and Legal Obligations	3
3.1	Governments	3
3.2	Corporations and Technology Providers	3
3.3	Developers and AI Researchers	3
4	Implementation and Compliance	3
4.1	Global Data Governance Framework	3
4.2	National Legislation	3
4.3	Public Awareness and Digital Literacy	3
5	Enforcement Mechanisms	4
5.1	Legal Accountability	4
5.2	Right to Data Portability	4
5.3	Whistleblower Protections	4

Preamble

Recognizing that digital technologies have become integral to modern life, and acknowledging the growing risks of data exploitation, digital surveillance, and cyber threats, this Declaration affirms the following principles:

1. Individuals have the inalienable right to control their digital identities and personal data.
2. Governments and corporations must adhere to transparent, ethical, and fair data collection and usage practices.
3. Digital sovereignty must be protected, ensuring users' rights across jurisdictions without unjustified surveillance or restrictions.
4. AI and automated decision-making systems must not undermine individual autonomy, privacy, or freedom of expression.
5. Cybersecurity and digital infrastructure must be designed to prevent harm, manipulation, and data breaches.

Article 1: Definitions

For the purposes of this Declaration:

- **Digital Sovereignty:** The right of individuals, communities, and nations to control their digital presence, data, and online activities.
- **Personal Data:** Any information that can be used to identify an individual, including biometric, behavioral, and digital metadata.
- **Algorithmic Governance:** The use of AI-driven systems to make decisions that impact individuals, communities, or institutions.
- **Data Exploitation:** The unethical or unauthorized collection, sale, or use of personal information for profit, surveillance, or manipulation.
- **Cybersecurity Rights:** Legal protections ensuring individuals' digital assets, communications, and personal data remain secure.

Article 2: General Principles

2.1 Right to Digital Ownership

Every individual has the right to own, manage, and control their personal data, including the right to access, modify, or delete information stored about them.

2.2 Data Privacy and Consent

Data collection must be based on explicit, informed, and revocable consent, ensuring individuals are aware of how their information is used.

2.3 Protection from Algorithmic Discrimination

AI and automated systems must be transparent, explainable, and free from bias that disproportionately impacts marginalized groups.

2.4 Right to Encryption and Security

Individuals have the right to use encryption and other security tools to protect their communications and data from unauthorized access.

2.5 Freedom from Mass Surveillance

Governments and corporations must not engage in mass data collection or surveillance without due legal process and transparent oversight.

Article 3: Ethical and Legal Obligations

3.1 Governments

States shall enact laws that protect digital rights, prevent unlawful surveillance, and hold corporations accountable for data misuse.

3.2 Corporations and Technology Providers

Companies must adhere to ethical data practices, provide transparency regarding data collection, and give users full control over their digital presence.

3.3 Developers and AI Researchers

Technology professionals must design systems that prioritize individual rights, fairness, and security, ensuring compliance with human rights standards.

Article 4: Implementation and Compliance

4.1 Global Data Governance Framework

An international regulatory body shall be established to monitor compliance with digital rights principles and recommend best practices.

4.2 National Legislation

Countries shall adopt digital rights laws that enforce ethical data use, cybersecurity protections, and algorithmic transparency.

4.3 Public Awareness and Digital Literacy

Governments and educational institutions shall promote digital literacy, ensuring individuals understand their rights and risks in the digital sphere.

Article 5: Enforcement Mechanisms

5.1 Legal Accountability

Entities violating digital sovereignty and privacy rights shall be subject to legal action, including penalties, sanctions, and reparations.

5.2 Right to Data Portability

Individuals must be able to transfer their data between platforms without restriction, ensuring autonomy over their digital lives.

5.3 Whistleblower Protections

Persons exposing unethical or illegal digital practices shall be protected from retaliation under international human rights law.

Final Provisions

This Declaration serves as a foundational ethical and legal framework for digital sovereignty and data rights. It shall be open to ratification by states, corporations, and institutions, who commit to upholding its principles.

Signed on February 27, 2025

Marie Seshat Landry
Marie Landry's Spy Shop
www.marielandryceo.com