

GLOBAL DIGITAL CITIZENSHIP DECLARATION

A Civilizational Contract for the Digital Age toward 2035

Draft for Discussion

“Borders may define states, but they should never define the value of a human life.”

Prepared under the auspices of the World Digital Economy Organization (WDEO)

Compiled and drafted by Jessica Sage (Li Wenyan), Digital Civilization Architect

Initial Draft: 16 July 2026

Vision Preamble

For nearly two centuries, humanity has continued to explore a common question: what kind of institutional order can genuinely advance human freedom, dignity, and civilizational progress?

Frédéric Bastiat reminded us that we must examine not only the visible benefits produced by institutions, but also their long-term and less visible consequences. Friedrich A. Hayek explained the importance of liberty, the rule of law, and spontaneous order to modern civilization. Franz Oppenheimer reconsidered the origins of the state and the legitimate purpose of public power.

Today, artificial intelligence, digital identity, data assets, and intelligent agents are reshaping the relationships between individuals and society, individuals and states, and humanity and the world. Human civilization is moving from industrial civilization toward digital civilization; from territorially bounded societies toward globally networked societies; from primarily physical identity toward digitally verifiable identity; and from nationally isolated governance toward global collaborative governance.

At this historic turning point, a new civilizational subject is emerging: the Global Digital Citizen.

Global digital citizenship is not a new nationality. It is a shared identity for the age of digital civilization. It does not seek to replace states. Rather, while respecting national sovereignty, it seeks to establish a more open, trustworthy, accountable, and cooperative human order.

The Global Digital Citizenship Declaration is therefore proposed as a new charter for the age of artificial intelligence, founded on human dignity, data sovereignty, global contribution, the spirit of contract, and civilizational responsibility. Its purpose is to help open a new era of digital civilization.

Preamble

Humanity is entering a new stage of civilization that transcends borders and connects the physical and digital worlds.

A person today may be born in one country, educated in another, employed in a third, and may pay taxes, social insurance, and healthcare contributions across several jurisdictions, while remaining continuously connected to global society through the internet, artificial intelligence, and digital platforms.

Yet existing institutions still define individuals primarily by nationality, territory, organizational affiliation, and traditional administrative boundaries:

- A.** Human contributions may be global, while rights remain fragmented across different countries.
- B.** Personal data continuously creates value, while only a small share of that value returns to the individual.
- C.** Human identity has become increasingly digital, while many governance systems remain rooted in the industrial age.
- D.** Artificial intelligence is beginning to act on behalf of individuals, yet no global consensus has emerged regarding its authority, responsibilities, and limits.

Humanity therefore needs a new civilizational contract.

This contract is not intended to abolish states or create a supranational power above them. It seeks, instead, to establish common principles for global mobility, digital identity, data rights, artificial intelligence, and future civilization, while respecting national sovereignty, cultural diversity, and the rule of law.

Global digital citizenship is not a new nationality. It is a verifiable digital identity, a sustainable framework of rights and responsibilities, a form of civilizational participation beyond geography, and a long-term institutional project belonging to all humanity.

Chapter I. Why Humanity Needs a New Civilizational Contract

Industrial civilization established a social contract centered on states, institutions, capital, and labor.

1. New Relations of Production in Digital Civilization

1. Data has become a major factor of production.
2. Algorithms participate in the allocation of resources.
3. Artificial intelligence participates in decision-making.
4. Digital platforms connect global society.
5. Individual contributions increasingly cross national and organizational boundaries.
6. Virtual space is becoming a second sphere of human life.

2. From Status-Based Governance to Contribution-Based Governance

2.1 Traditional institutions primarily ask: To which country, organization, or administrative unit does a person belong?

2.2 Digital civilization must also ask: What value has a person created for the world?

2.3 Future societies should not assess human worth solely on the basis of birthplace, passport, wealth, office, or institutional rank. They should gradually establish more transparent, fair, and verifiable systems for recognizing contribution.

2.3.1 Borders may define the jurisdiction of states, but they should never define the value of human life.

2.3.2 Identity may have territorial attributes, but human dignity must not be territorially limited.

2.3.3 Rules should apply to all actors without exception based on power, wealth, or position.

2.3.4 Technological progress must be translated into greater human freedom, dignity, and opportunity.

2.3.5 Global governance must ensure the equal participation of both developed and developing countries.

2.3.6 Digital civilization must not create new privileged classes or structures of digital colonialism.

2.3.7 Humanity should move from identity-based governance toward contribution-based governance, and from ownership-based governance toward trusteeship-based governance.

2.3.8 A new civilizational contract should rest on five foundations: trustworthy identity, data autonomy, verifiable contribution, parity between rights and responsibilities, and technology for human good.

Chapter II. Digital Identity

Digital identity is the foundational expression of legal and personal identity in digital civilization. It is neither a platform account nor a single electronic document issued by one government. It is a system of identity that is controlled by the individual, verifiable, authorizable, revocable, and interoperable across systems.

1. Identity Belongs to the Individual

1.1 Every person should retain fundamental control over their digital identity.

1.2 Governments, companies, platforms, and international organizations may verify identity in accordance with law, but must not unconditionally possess, sell, or misuse personal identity information.

2. One Person, One Core CODE, Multiple Contexts

2.1 Every natural person may possess one trusted and verified core identity - a digital identity access credential - and may generate context-specific credentials for education, healthcare, employment, finance, and social services.

2.2 The core identity should remain encrypted, stable, and globally usable, while contextual credentials may be updated dynamically.

3. Minimum Necessary Disclosure

3.1 Any institution verifying identity should receive only the information strictly necessary for the specific transaction or purpose.

3.2 Proof that a person is over eighteen should not require disclosure of the person's complete date of birth.

3.3 Proof of a qualification should not require disclosure of a person's full educational and employment history.

4. Portability and Mutual Recognition

4.1 Digital identity should be mutually recognizable across countries, platforms, and institutions under lawful authorization and common security standards.

4.2 Digital identity should accompany the individual and must not be locked into a single platform, company, or jurisdiction.

5. Parallel Recognition of Natural Persons, Institutions, and AI Subjects

5.1 A global digital citizenship framework may include:

- 5.1.1 Natural-person digital citizens;
- 5.1.2 Corporate digital citizens;
- 5.1.3 Civil-society and nonprofit digital citizens;
- 5.1.4 Public-institution digital citizens;
- 5.1.5 AI agents and other digital subjects.

5.2 Different categories of subjects shall have different rights, obligations, authentication requirements, and boundaries of responsibility.

6. Digital Identity Wallet - A Global Citizen Passport

6.1 Digital identity may be carried through a personal digital wallet.

6.2 The wallet may store or invoke:

- 6.2.1 Decentralized identifiers;
- 6.2.2 Verifiable credentials;
- 6.2.3 Proofs of access to public services;
- 6.2.4 Educational and professional qualifications;
- 6.2.5 Authorization records;
- 6.2.6 Data-use permissions;
- 6.2.7 Records of global contribution;
- 6.2.8 Delegated authority granted to AI agents.

The Global Citizen Digital Passport, or digital wallet, is not a centralized repository of raw personal data. It is a personally controlled gateway for identity credentials, authorization keys, and access rules.

Chapter III. Global Contribution Ledger

Future societies should record not only wealth, but also contribution. The Global Contribution Ledger is a mechanism for credibly recording the contributions of individuals, institutions, and intelligent systems to the public good, knowledge creation, social service, ecological protection, technological innovation, cultural exchange, and civilizational development.

The Global Contribution Ledger must not become a new social hierarchy or a single-dimensional social-credit score. It should be multidimensional, transparent, voluntary, appealable, and auditable.

1. Principal Dimensions of Contribution

- 1.1 Knowledge Contribution: Scientific research, education, open knowledge, innovation, and public communication.
- 1.2 Social Contribution: Volunteer service, community development, support for vulnerable groups, and participation in public affairs.
- 1.3 Ecological Contribution: Energy conservation, emissions reduction, environmental protection, the circular economy, and ecosystem restoration.

- 1.4 Economic Contribution: Entrepreneurship, job creation, taxation, social-insurance payments, and sustained productive activity.
- 1.5 Health Contribution: Public-health promotion, voluntary sharing of health data, and participation in medical research.
- 1.6 Civilizational Contribution: Intercultural exchange, peaceful cooperation, digital ethics, and innovation in public institutions.
- 1.7 Technological Contribution: Open-source software, algorithmic safety, infrastructure development, and the diffusion of inclusive technology.

2. Contribution Does Not Confer Power

- 2.1 Contribution records must not grant any individual privileges above the law.
- 2.2 Contribution may justify reasonable recognition, opportunity, or public benefit, but must never become a means of purchasing political power, judicial immunity, or claims of superior human worth.

3. Contributions May Accumulate Across Borders

- 3.1 When a person pays taxes or social-insurance contributions, creates employment, shares knowledge, or serves the public good in different countries, those records should not be entirely severed by cross-border mobility.
- 3.2 The Global Contribution Ledger should connect, where legally possible, with national systems and create verifiable cross-border proofs of contribution while respecting territorial law.

4. Contribution Records Must Be Contestable

- 4.1 Any contribution record affecting a person's substantial rights or opportunities must include:
 - 4.1.1 Disclosure of the data source;
 - 4.1.2 An explanation mechanism for relevant algorithms;
 - 4.1.3 A channel for human review;
 - 4.1.4 A procedure for objection and appeal;
 - 4.1.5 Mechanisms for correction and deletion.

Chapter IV. Data Sovereignty

Data arises from human behavior, relationships, labor, health, consumption, mobility, and creativity. It has personal characteristics and may also possess corporate value, public value, and national-security significance.

Data sovereignty is therefore not the absolute ownership of data by a single actor. It is a layered structure of rights that distinguishes personality rights, rights of use, management authority, rights to benefit, and public responsibilities.

1. Personality Rights in Personal Data

1.1 Data closely related to identity, health, thought, communications, location, and behavior should first be protected as an extension of the individual.

1.2 Every person should enjoy:

1.2.1 The right to be informed;

1.2.2 The right of access;

1.2.3 The right to correction;

1.2.4 The right to deletion;

1.2.5 The right to authorize use;

1.2.6 The right to withdraw authorization;

1.2.7 The right to portability;

1.2.8 The right to know whether value or revenue is generated;

1.2.9 The right to object to automated decision-making.

2. Data Use Requires Genuine Authorization

2.1 Institutions must not substitute lengthy, ambiguous, or coercively bundled terms for genuine consent.

2.2 Authorization should clearly state:

2.2.1 What data will be used;

2.2.2 For what purpose;

2.2.3 For how long it will be retained;

2.2.4 Whether it will be shared with third parties;

2.2.5 Whether it will be used to train AI systems;

2.2.6 Whether it will generate commercial revenue;

2.2.7 How authorization may be withdrawn.

3. Fair Distribution of Data-Derived Value

3.1 Where personal data continuously contributes to platform revenue, model training, commercial analysis, or asset formation, reasonable mechanisms for value sharing should be explored.

3.2 Data-derived benefits may take the form of:

3.2.1 Direct financial returns;

3.2.2 Credits for public services;

3.2.3 Healthcare and educational benefits;

3.2.4 Supplementary social protection;

3.2.5 Returns from digital assets;

3.2.6 Public data dividends.

3.3 The distribution of data-derived value must guard against speculation, financial abuse, and new forms of digital inequality.

4. National Data Sovereignty

4.1 The global digital citizenship framework must respect national data sovereignty and territorial law. In principle:

4.1.1 Raw sensitive data should remain within its lawful jurisdiction;

4.1.2 Each country should retain lawful control over access and decryption relating to data within its jurisdiction;

4.1.3 Cross-border transfers should follow clear and enforceable rules;

4.1.4 No international institution should centrally possess the world's raw personal data;

4.1.5 Global mutual recognition should operate primarily through standards, keys, credentials, proofs, and authorization mechanisms.

5. Mathematical Mapping and Distributed Storage

5.1 Future research may explore high-dimensional mathematical mapping, cryptography, distributed verification, zero-knowledge proofs, and privacy-enhancing computation to reduce the risks created by centralized cross-border aggregation of raw data.

5.2 The concept of a 'four-dimensional mathematical storage space' should be treated as a research direction requiring scientific validation, not as an established technical standard.

5.3 Future research should address:

5.3.1 Data-mapping and encoding rules;

5.3.2 Key generation and recovery mechanisms;

5.3.3 Separation of decryption authority;

5.3.4 Security of distributed nodes;

5.3.5 Cryptographic security in the quantum era;

5.3.6 Disaster recovery and long-term preservation;

5.3.7 Public auditability and algorithmic transparency.

Chapter V. Contract Civilization

Digital civilization cannot rely solely on commands backed by power, nor solely on platform rules. It must gradually move from a society based on status and dependence toward a contract civilization characterized by clear rights and responsibilities, transparent procedures, and verifiable commitments.

Contract civilization means that the sources of power must be clear; public office must have defined responsibilities; enterprises using data must assume corresponding obligations; platforms making rules must provide channels for appeal; AI acting on behalf of a person must be duly authorized; and all significant commitments should be recordable, traceable, and auditable.

1. No Digital Privilege Above the Rules

- 1.1** No state, institution, enterprise, officeholder, or technology platform should be exempt from responsibility merely because it controls power, capital, or data.
- 1.2** Exclusive access channels, preferential allocation of public resources, internal privileges, and opaque decisions should, where public resources are involved, be reviewed for legitimacy, necessity, and proportionality.

2. Public Office Is a Public Contract

- 2.1** Public power is not personal property. It is a responsibility entrusted by the people, law, and institutions. Likewise, funds, data, and resources managed by corporate leaders are not equivalent to their personal property.
- 2.2** Management authority must be constrained by:
 - 2.2.1** Defined limits of authorization;
 - 2.2.2** Disclosure requirements;
 - 2.2.3** Conflict-of-interest review;
 - 2.2.4** Financial audit;
 - 2.2.5** Traceable accountability;
 - 2.2.6** Term limits and exit mechanisms.

3. Smart Contracts Cannot Replace Legal Justice

- 3.1** Smart contracts may improve execution efficiency, but code must not automatically acquire a status superior to law and human rights.
- 3.2** Any automated contract affecting life, liberty, property, health, or access to essential services must preserve channels for human review and effective remedy.

Chapter VI. Trusteeship Civilization

Future civilization must reconsider the relationship between ownership and management. Governments manage public resources; banks manage deposits; platforms manage data; funds manage capital; enterprises manage the fruits of labor; and artificial intelligence increasingly manages information and decision processes.

These forms of authority are fundamentally fiduciary or trusteeship-based. The central principle of trusteeship civilization is that control over resources does not confer unlimited authority to dispose of them.

1. Power as a Trusteeship Responsibility

Public administrators should serve the public interest and must not use office to establish permanent privilege.

2. Capital as a Trusteeship Responsibility

Funds managed by financial institutions largely belong to depositors, investors, pension participants, and the broader public. Financial managers must therefore owe duties of loyalty, prudence, transparency, and risk control.

3. Data as a Trusteeship Responsibility

3.1 The fact that platforms or institutions hold personal data does not mean that they own the person.

3.2 Data controllers should assume trustee-like duties and must not:

3.2.1 Secretly repurpose data;

3.2.2 Collect data excessively;

3.2.3 Use technological superiority to harm individuals;

3.2.4 Discriminate through opaque algorithms;

3.2.5 Unreasonably prevent individuals from transferring their data.

4. Foundations as Civilizational Trustees

4.1 Foundations serving digital civilization should pursue long-term public benefit, including:

4.1.1 Inclusive access to technology;

4.1.2 Digital education;

4.1.3 Capacity-building in the Global South;

4.1.4 Research on AI ethics;

4.1.5 Protection of data rights;

4.1.6 Digital public infrastructure;

4.1.7 Intergenerational civilizational responsibility.

4.2 Foundation assets are not the private assets of founders or managers.

4.3 Every foundation should maintain independent governance, audit, conflict-of-interest controls, and public transparency.

Chapter VII. AI Agents and Digital Governance

AI agents will increasingly act as digital representatives of individuals, enterprises, and public institutions. They may conduct information retrieval, execute transactions, issue medical reminders, plan education, obtain cross-border services, negotiate contracts, submit public-service applications, grant data permissions, and manage assets.

AI agents must therefore be incorporated into a clear framework of rights, authority, and responsibility.

1. AI Agents Must Be Identifiable

1.1 Any AI agent that materially affects a person must possess a verifiable identity.

1.2 Every citizen has the right to know:

- 1.2.1 Whether they are interacting with a human or an AI system;
- 1.2.2 On whose behalf the AI is acting;
- 1.2.3 What authority the AI has received;
- 1.2.4 What data the AI has accessed or invoked;
- 1.2.5 Who bears responsibility for the resulting decision or action.

2. AI Agents Require Limited and Revocable Authorization

- 2.1 An AI agent may act on behalf of a person or institution only within a clearly defined scope.
- 2.2 An encrypted authorization system for AI agents should specify:
 - 2.2.1 The subject matter and scope of authority;
 - 2.2.2 Financial limits;
 - 2.2.3 Time limits;
 - 2.2.4 Permitted data categories;
 - 2.2.5 Geographic limits;
 - 2.2.6 A revocation mechanism;
 - 2.2.7 An emergency-stop mechanism.

3. Responsibility Cannot Be Transferred to an Algorithm

- 3.1 AI must not become a means of evading responsibility.
- 3.2 Where AI causes substantial harm, responsibility should be allocated according to the circumstances among:
 - 3.2.1 Developers;
 - 3.2.2 Deployers;
 - 3.2.3 Users;
 - 3.2.4 Data providers;
 - 3.2.5 Auditors and regulators.

4. Human Final Control over High-Risk Decisions

- 4.1 Major decisions involving justice, medicine, warfare, public safety, financial freezing, social protection, children's rights, or fundamental human rights must not be made entirely by AI.
- 4.2 Human beings must retain meaningful powers of supervision, explanation, intervention, and final veto.

5. Global Standards for AI-Agent Governance

- 5.1 Future governance should advance:
 - 5.1.1 Global identity standards for AI agents;
 - 5.1.2 Machine-verifiable authorization protocols;
 - 5.1.3 Cross-platform interoperability of agents;
 - 5.1.4 Auditable logs of AI behavior;

- 5.1.5 AI liability insurance;
- 5.1.6 Registration systems for high-risk AI;
- 5.1.7 Human emergency-takeover mechanisms.

Chapter VIII. From Earth Citizenship to Cosmic Citizenship

Digital citizenship is not the endpoint of civilization. As humanity gradually establishes a presence on the Moon, Mars, space stations, and in deep space, traditional systems based on nationality, territory, and geography will face new challenges.

Future human beings may simultaneously possess national citizenship, global digital citizenship, membership in an extraterrestrial community, scientific or space-mission status, and an AI-enabled symbiotic digital identity.

The purpose of cosmic citizenship is not to abandon Earth, but to enlarge the boundaries of human responsibility.

1. Earth as the Common Cradle of Civilization

No country, enterprise, or organization entering outer space should disregard Earth's ecology or the interests of humanity as a whole.

2. Outer Space Must Not Reproduce Earth's Structures of Privilege

Humanity must not reproduce colonialism, monopoly, resource plunder, or extreme inequality in outer space.

3. Space Resources Should Be Governed by Trusteeship Principles

The development of resources on the Moon, Mars, asteroids, and other celestial bodies should take account of scientific research, intergenerational equity, environmental protection, peaceful use, and the common interests of humanity.

4. Cosmic Civilization Requires New Ethics

Future humanity will need to consider the identity of persons born beyond Earth; labor rights in space; interplanetary social protection; the legal and ethical status of AI and robotic entities; the governance of extraterrestrial resources; relations between Earth and off-world communities; and the long-term survival of human civilization.

Chapter IX. Global Governance Blueprint 2035

The global digital citizenship framework should be built through an open, multilateral, phased, and verifiable process. The World Digital Economy Organization may propose itself as one of the initiating, coordinating, and secretariat candidate institutions for the Global Digital Citizenship Initiative, while promoting cooperation among international organizations, governments, technical communities, enterprises, universities, and civil society.

No global governance authority should be permanently monopolized by a single institution.

1. Overall Governance Structure

Layer One: Global Digital Citizenship Council

The Council should include participating states, international organizations, technical standard-setting bodies, development institutions, civil-society representatives, and independent experts.

Its principal responsibilities should include reviewing global digital citizenship principles; establishing frameworks of rights and responsibilities; coordinating cross-border recognition of identity; supervising mechanisms for data-derived value; reviewing AI-agent governance standards; protecting the equal participation of developing countries; and preventing technological or institutional monopolies.

Layer Two: Specialized Committees and Working Groups

1. Digital Identity and Wallet Working Group
2. Data Sovereignty and Privacy Working Group
3. Mathematical Encoding and Cryptography Working Group
4. AI-Agent Governance Working Group
5. Digital Literacy and Ethics Working Group
6. Law, Policy and Human Rights Working Group
7. Data Value and Benefit-Sharing Working Group
8. Global South and Inclusive Development Working Group
9. Earth and Cosmic Civilization Research Committee

Layer Three: Regional Pilot Networks

Compatibility pilots should be developed in accordance with existing regional institutions, including in Asia, Europe, the Middle East, Africa, the Americas, small-island states, and among cross-border mobile populations.

2. Principal International Partners and Suggested Roles

- 2.1 World Digital Economy Organization (WDEO): Overall initiative coordination; construction of a multilateral cooperation platform; mechanisms for participation by the Global South; drafting of conventions and white papers; organization of cross-institutional expert committees; coordination of regional pilots; research on data-value distribution; and advancement of the long-term digital civilization agenda. WDEO should establish international credibility through open governance, independent audit, conflict-of-interest controls, and multistakeholder participation.
- 2.2 United Nations and the United Nations Development Programme (UNDP): Potential fields of cooperation include alignment with the United Nations Global Digital Compact and related agendas; inclusive digital development; digital infrastructure in developing countries; reduction of the digital divide; support for public-development projects; and policy dialogue among Member States.
- 2.3 United Nations Educational, Scientific and Cultural Organization (UNESCO): Potential fields of cooperation include digital citizenship literacy, AI ethics, digital education, online civic culture,

youth protection, global digital citizenship curricula, and infrastructure development in underserved regions.

- 2.4 International Telecommunication Union (ITU): Potential fields of cooperation include communications infrastructure, network interoperability, green computing, technical security, AI identity and trust, distributed nodes, and digital access in developing countries.
- 2.5 World Wide Web Consortium (W3C): Potential fields of cooperation include decentralized identity, verifiable credentials, digital-wallet compatibility, web-identity standards, minimum disclosure, and cross-platform identity interoperability. W3C is well suited to provide open technical standards, but should not be responsible for approving global citizenship status or managing raw personal data.
- 2.6 Organisation for Economic Co-operation and Development (OECD): Potential fields of cooperation include AI governance policy, data governance, trusted data flows, compliance research for advanced economies, taxation, labor, and digital-economy policy, and compatibility with existing international principles. OECD experience is valuable, but global institutional design must also protect the equal voice of non-OECD countries and the Global South.
- 2.7 European Digital Identity Wallet: Potential fields of cooperation include European wallet practice, cross-border recognition of electronic identity, credential operations and user protection, and interface-compatibility research with a global digital citizenship framework. The global framework should not replace existing European systems, but should reduce duplication through technical compatibility and mutual recognition of protocols.
- 2.8 Other Regional Organizations: Research and dialogue may gradually be developed with the African Union, the Association of Southeast Asian Nations, the Gulf Cooperation Council, the Organization of American States, the Council of Europe, regional development banks, and organizations serving migrant and cross-border workers.

3. Principles of International Coordination

- 3.1 Build on Existing Systems: The framework should build on existing decentralized identifiers, verifiable credentials, digital wallets, privacy protections, and cross-border data rules rather than attempting to replace them.
- 3.2 Territorial Management of Sensitive Data: Raw sensitive data should, in principle, remain within its lawful jurisdiction. Global recognition should rely on credentials, authorization, proofs, and key-management mechanisms.
- 3.3 Multilateral Governance: No single state, enterprise, or organization should monopolize digital identity, global contribution records, or rules for distributing data-derived value.
- 3.4 Equal Participation of Developing Countries: Institutional design must not be dominated solely by technologically advanced states and developed economies.
- 3.5 Open Verification: Core standards, algorithms, and governance rules should be subject to review by independent experts, the public, and participating states.

4. Phased Roadmap

Phase I: 2026-2027 - Theory and Initiative Publish the Global Digital Citizenship Declaration; complete a white paper; establish an international expert network; launch a thematic initiative through AI for Good; conduct research on digital identity, the Global Contribution Ledger, and data-value sharing; and propose a framework for multilateral memoranda of cooperation.

Phase II: 2027-2030 - Standards and Pilots Conduct compatibility testing for digital wallets; establish pilots for natural-person and institutional digital citizenship; promote cross-border recognition of educational, professional, and public-service credentials; test data authorization and value-sharing mechanisms; pilot delegated authorization for AI agents; and build capacity in the Global South.

Phase III: 2030-2033 - Regional Mutual Recognition Establish multiple regional networks for mutual recognition of digital identity; expand cross-border use of contribution proofs; establish dispute-resolution mechanisms for digital citizenship; broaden pilots for institutional digital citizens and AI-agent governance; and launch public-service interfaces for global digital citizenship.

Phase IV: 2033-2035 - Global Collaboration Advance an open global protocol for digital citizenship; establish a multilateral governance council; achieve compatibility among major regional standards; establish mechanisms for data-derived value and public digital dividends; and formulate a long-term governance agenda for Earth and cosmic civilization.

Chapter X. An Initiative for the United Nations AI for Good

We call upon the United Nations, international organizations, national governments, technical standard-setting bodies, enterprises, universities, and civil society to jointly launch a Global Digital Citizenship Cooperation Initiative.

The Initiative should not create a new center of power. It should establish a framework for cooperation across countries, institutions, and technology platforms.

We propose that the AI for Good platform advance the following ten actions:

1. Establish a Global Digital Citizenship Task Force: Conduct interdisciplinary research on digital identity, data rights, global contribution, AI agents, and digital governance.
2. Publish Global Digital Citizenship Principles: Develop a common value framework for individuals, governments, platforms, enterprises, and AI systems.
3. Create a Digital Identity Interoperability Laboratory: Research compatibility among decentralized identifiers, verifiable credentials, digital wallets, and regional identity systems.
4. Establish a Trusted Identity Framework for AI Agents: Ensure that AI agents are identifiable, authorized, auditable, stoppable, and accountable.
5. Launch a Global Contribution Ledger Pilot: Prioritize contributions in education, public service, ecology, scientific research, and intercultural cooperation.
6. Explore Mechanisms for Sharing Data-Derived Value: Enable individuals and society to receive a fair share of the benefits generated by the data economy and AI development.

7. Protect the Rights of Globally Mobile Populations: Study the portability of education, professional qualifications, social insurance, healthcare, and digital services across borders.
8. Establish a Global South Participation Fund: Support developing countries in building digital infrastructure, training digital talent, and participating in international rule-making.
9. Launch a Digital Civilization Youth Programme: Enable young people to participate in AI ethics, digital public policy, and the design of future civilization.
10. Publish the Global Digital Citizenship Roadmap 2035: Develop open, inclusive, and trustworthy infrastructure for global digital civilization through joint research, regional pilots, technical standards, and public-policy cooperation.

Chapter XI. Civil Society and Intellectual Dialogue Network

A global digital citizenship framework requires the participation of governments and international organizations, but it also requires sustained dialogue with civil society, trade unions, cooperatives, technical communities, open-source organizations, and decentralized social movements.

Research on grassroots democracy, local autonomy, worker self-management, anti-monopoly thought, and decentralized governance may draw upon case studies including, but not limited to, the International of Anarchist Federations; FAU Switzerland; the Federation of German-speaking Anarchists; FAU Germany; the Fédération Anarchiste; the Federazione Anarchica Italiana; the Federación Anarquista Ibérica; and the Anarchist Federation in the United Kingdom.

These organizations may serve as sources for examining decentralized governance, grassroots participation, and resistance to the concentration of power. Nevertheless, the global digital citizenship framework must adhere to peace, the rule of law, human rights, open governance, and nonviolence.

No ideology or organization should automatically acquire governing legitimacy merely because it opposes centralized power. Equally, no state or large institution should be exempt from public scrutiny merely because it already possesses authority.

Chapter XII. Conclusion

Global digital citizenship does not seek to deprive people of national citizenship. It seeks to ensure that, in addition to national identity, every person may possess a civilizational identity oriented toward humanity as a whole.

1. It does not deny sovereignty; it seeks a new balance among sovereignty, human rights, data rights, and global responsibility.
2. It does not oppose technology; it requires technology to remain subject to ethics, law, and human dignity.
3. It does not seek to abolish wealth; it requires wealth, power, data, and algorithms to bear responsibilities proportionate to their influence.
4. We do not seek a digital world in which a small number of institutions control everyone.

5. We seek a digital civilization in which identity belongs to the individual, data is protected, contribution is recognized, power is constrained, AI serves humanity, and states cooperate with one another.
6. Global digital citizenship is not a fantasy about the future. It is a new contract that humanity must begin to discuss in response to the digital age.

Technology can change the world, but only civilization can determine where the world is going.

Chapter XIII. Intellectual Foundations and Drafting Methodology

The Global Digital Citizenship Declaration systematically sets out the vision, identity, rights, responsibilities, governance mechanisms, international cooperation, and 2035 development blueprint of global digital citizenship. It is grounded in the civilizational transition brought about by artificial intelligence and draws on the long-term work of Franz Oppenheimer, Friedrich August von Hayek, and Frédéric Bastiat concerning state power, the rule of law, economic choice, and individual liberty.

1. Intellectual Foundations

1.1 Franz Oppenheimer (1864-1943) was a German sociologist, political economist, and physician.

In *The State*, he examined state formation from historical and sociological perspectives and distinguished the 'economic means' of creating wealth through labor and exchange from the 'political means' of acquiring resources through coercion and conquest. His work encourages renewed examination of the sources, limits, and public responsibilities of state power.

1.2 Friedrich August von Hayek (1899-1992) was an Austrian-born British economist, political philosopher, and Nobel laureate. In *The Constitution of Liberty*, he systematically examined individual freedom, general rules, the rule of law, and spontaneous order. He emphasized that public power must be constrained by stable rules and that civilizational progress depends on dispersed knowledge, freedom of choice, and institutional humility.

1.3 Frédéric Bastiat (1801-1850) was a French economist, political thinker, and legislator. In *What Is Seen and What Is Not Seen*, he argued that policy must be assessed not only by its immediate and visible benefits, but also by its long-term costs, opportunity losses, and less visible effects on other groups. This principle offers important guidance for evaluating digital platforms, AI decisions, the allocation of public resources, and the data economy.

These thinkers differed in period, discipline, and specific doctrine, but their work converges on a fundamental proposition: states and institutions should serve human freedom and dignity; power must be constrained by law and responsibility; and economic and social decisions must account for both visible outcomes and invisible costs.

The Declaration is not a simple compilation of these works. It re-examines their central questions under contemporary conditions in which artificial intelligence, digital identity, data sovereignty, AI agents, and global mobility have become realities.

Guided by the principle that 'borders may define states, but they should never define the value of a human life,' the Declaration seeks to establish a new civilizational contract among national sovereignty, individual liberty, the public interest, and global cooperation.

2. Drafting Form and Normative References

In structure and expression, this Declaration draws on the general drafting practices of the Charter of the United Nations, major declarations of the United Nations system, and international conventions. It adopts the following framework:

- 2.1 A preamble explaining the historical context, common values, and purpose of the initiative;
- 2.2 Principles and provisions defining the fundamental rights, responsibilities, and governance boundaries of digital citizens;
- 2.3 Separate chapters addressing digital identity, global contribution, data sovereignty, contract civilization, trusteeship responsibility, and AI governance;
- 2.4 Cooperation mechanisms and an implementation roadmap linking values, institutional design, and international action;
- 2.5 Normative language such as 'shall,' 'should,' 'must not,' 'recognizes,' 'respects,' and 'promotes,' in order to strengthen institutional precision;
- 2.6 A clear distinction among value principles, policy initiatives, technical standards, and future research directions, so that unverified concepts are not presented as established international rules;
- 2.7 Recognition that, at its present stage, the Declaration is a civilizational initiative and normative framework addressed to global society and does not have the legally binding force of an international treaty. Its long-term objective is to develop, through the participation of international organizations, governments, technical standard-setting bodies, academia, enterprises, and civil society, into a global digital citizenship framework that can be debated, verified, piloted, and gradually supported by international consensus.

World Digital Economy Organization (WDEO) Secretariat

Compiled and drafted by Jessica Sage (Li Wenyan), Digital Civilization Architect

Initial Draft: 16 July 2026