DATA GOVERNANCE PRINCIPLES *for the* GLOBAL DIGITAL ECONOMY

DATA HAS BECOME A CRITICAL RESOURCE DRIVING INNOVATION AND ECONOMIC GROWTH WORLDWIDE. The free exchange of data has facilitated unprecedented choice, opportunity, and mobility to people around the world, created new industries and jobs, and raised global standards of living.

Data can also be exploited by malicious actors or cause unintended harm to individuals and societies. But the collection and use of data are not inherently dangerous or harmful. Limitations on data use should be tailored and proportional to manage specific and meaningful risks. The first goal of policymaking is to facilitate the safe and responsible use of data to improve people's lives.

The architecture of global data governance is comprised of an interlinked set of laws, conventions, protocols, and standards at the international, regional, national, and local levels. Gaps in this architecture have resulted in a lack of clarity that is undermining confidence in and adoption of new technologies and limiting the tools available to address harmful uses of data.

A unified approach to develop data governance frameworks and integrate them into this global architecture is needed. Risk-based governance structures can enable innovation and competition and protect people from harm. These structures must be flexible, consistent, and interoperable.

Countries around the world recognize the benefits of creating clear data governance rules to enable innovation and development while protecting their citizens from harm. Many are establishing legal and regulatory frameworks to govern data. While national data governance regimes are essential to promote innovation and reflect local values, culture, and customs, the global and integrated nature of the digital economy requires a common baseline of data governance principles on which national data governance regimes can be built.

A unified approach to develop data governance frameworks and integrate them into this global architecture is needed.

International rules, norms, laws, and frameworks governing data exist but are inadequate to address the needs of an increasingly digital society. Many focus on privacy and data protection but do not always address broader risks around data. In the absence of proper governance, data or restrictions on data can limit people's mobility and access to services, serve as a barrier to trade or anti-competitive "moat" that limits consumer choice, undermine the rule of law and public safety, or enable discrimination.

Existing frameworks often emphasize the rights of personal data subjects, with little attention to the rights and equities of other stakeholders. They are largely premised on rights of data ownership and privacy, and often treat consent as a sufficient condition for virtually unlimited exploitation of personal data. This places a significant burden on the individual to manage his or her digital footprint when they may lack the skills and tools to do so effectively.

Current frameworks are also based primarily on controlling access to data, as opposed to establishing risk-based protections again the misuse of data. Attempting to control access to data can limit innovation in important fields like health care and education. This approach also provides few protections against misuse of data once it has been "given away" or "shared."

Establishing common global principles and fostering a shared understanding of their implications is essential.

Furthermore, many existing frameworks are largely limited to personal data. While protection of personal data is important, non-personal data and "anonymized" or "de-identified" data will also play an increasingly important role in societies and economies. This will only become more important with the growth of machine-to-machine communications and the internet of things (IoT). Data governance structures must be designed to adapt to this future, capable of addressing risks around both "personal" and "non-personal" data. These structures must speak to concerns beyond privacy and provide clear guidelines to facilitate responsible sharing and use of data.

Existing data governance frameworks also lack transparency, as well as institutions and standards to allow for effective enforcement of global norms. Data plays an increasingly central role in every part of global affairs, including innovation, trade, criminal justice, national security, and mobility and migration.

Establishing common global principles and fostering a shared understanding of their implications is essential. Effective enforcement will require the incorporation of these data governance principles into both existing and new national laws and regulations, international institutions, trade agreements, bilateral and multilateral treaties, and global standards.

Recognizing the need to close these gaps in the global architecture of data governance, we resolve to address these challenges based on the following shared principles.

We affirm that national and international data governance frameworks should support the following objectives to:

1. **empower people and societies to make informed choices** about how digital data is generated, used and shared;
2. **protect human rights,** including the right to privacy, against infringement, and utilize data and digital systems to promote citizens' rights; and
3. **safeguard the ability of innovators, entrepreneurs and service providers** to collect, share, and use data, as long as they do not violate any of these other principles.

We further call for these frameworks to be risk-based, appropriately tailored, and include specific mechanisms to:

1. **preserve the free flow of data across borders** and between jurisdictions, and protect the mobility of people, goods, and services;
2. **facilitate the portability of data and ensure the interoperability of digital systems** around the world, as well as compliance with global standards;
3. **provide meaningful transparency and accountability** and enable the enforcement of rights;
4. **hold data processors responsible for the security and integrity** of data and digital systems;
5. **reflect the needs of a diverse range of stakeholders,** including private industry, civil society, and governments;
6. **discourage data practices that serve as a barrier** to fair and open competition; and
7. **provide that data processors respect all laws and regulations,** and the unique culture and customs, of all jurisdictions in which they operate, irrespective of location in which data is collected, stored, processed or used, as long as those laws or customs do not violate any of the above principles.

Produced thanks to the generous support of the Omidyar Network to the CSIS Technology Policy Program and the CSIS Project on Prosperity and Development.