Cross-Border Data Flows Enable the Digital Economy

The growth of e-commerce, digital services and the internet in general at a *national level* is supported by flexible approaches to the flow of data *internationally*. Allowing free flow of data across borders provides consumers with access to the global range and quality of services, and permits businesses to reduce their costs and prices for customers. It also delivers social and economic benefits to individuals, businesses and governments more rapidly by allowing the digital economy to flourish.

In a regulatory environment that allows data to flow, businesses are able to operate, to innovate and to access solutions and support anywhere in the world. For example:

- Services can emerge and be adopted in one national market, then expand readily to other markets, bringing benefits for consumers and businesses;
- Small businesses can open with a global reach from Day 1 by establishing an internet presence which is simultaneously national and international;
- Internet infrastructure suppliers, such as cloud computing providers and mobile operators, can structure their services to serve large numbers of clients in multiple markets at the lowest overall cost; and
- Businesses can scale up (and down) at critical points in their development making direct or indirect use of cloud and SaaS (Software as a Service) providers.

The strategic role of cross-border data flows has been recognised by policymakers:

UNCTAD[1] quotes McKinsey Global Institute:

"The international dimension of flows [of goods, services and finance has] increased global GDP by approximately 10 percent, equivalent to a value of $7.8 trillion in 2014. Data flows represent an estimated $2.8 trillion of this added value."

European Commission[3]:

"Unjustified restrictions on the free movement of data are likely to constrain the development of the EU data economy [...] risk fragmenting the market, reducing the quality of service for users and the competitiveness of data service providers, especially smaller entities."

OECD[2]:

"Cross-border data flows have increased economic efficiency and productivity, raising welfare and standards of living."

International Chamber of Commerce (ICC)[4]:

"ICC urges governments to ensure all citizens and companies can realize the full potential of the Internet [...] by adopting policies that facilitate the adoption of new technologies and global movement of data that supports them."

1. United Nations Conference on Trade and Development (UNCTAD), Data Protection Regulations and International Data Flows, 2016.
2. OECD, Internet Economy 2012. Paper 143.
3. European Commission, Communication on Building a European Data Economy, 2017.
4. ICC, Trade in the Digital Economy: A Primer on Global Data Flows for Policymakers, 2016.

Cross-border flows of data are currently regulated by a number of international, regional and national instruments and laws intended to protect individuals' privacy, the local economy or national security.

Cooperation between countries and regions could see widespread adoption of convergent approaches to data privacy and mechanisms for cross-border data flows. Not only could this improve privacy protection for individuals, but it could also stimulate data-driven economic activity across the entire region.

National data privacy regimes should be based on shared, core principles and provide flexibility in implementation

The mobile industry recognises that regulation of data privacy, including of cross-border data flows, is necessary. This should consistently provide consumers with confidence in existing and new services without limiting service adoption or imposing significant additional costs on service providers.

To achieve this, it is crucial for privacy regulation to be based on shared core principles which sit "at the heart of most national [privacy] laws and international regimes[5]" as well as industry initiatives. This would allow companies to treat data consistently across their operations, innovate more rapidly, achieve larger scale and reduce costs. Consumers will benefit from wider choice, improved service quality and lower prices of services.

The 2009 Madrid Resolution[6], for example, encourages consistent international protection of personal data and embraces privacy approaches from all five continents to facilitate "the international flows of personal data needed in a globalized world."

The Madrid Resolution advocates six privacy principles to be adopted by policymakers:

Lawful & fair	Purpose	Proportionate	Quality	Openness	Accountable
Personal data must be lawfully and fairly processed	Processing should be limited to specified purposes	Processing should be proportionate and not excessive	Data held should be accurate	The processor should be open regarding their activities	The processor should be accountable for their activities

Similar principles are reflected repeatedly in laws and policy initiatives around the world such as the Council of Europe Convention 108, the OECD Guidelines, the EU General Data Protection Regulation, the US Federal Trade Commission's Fair Information Practice Principles and the APEC Privacy Framework. The mobile industry has also adopted the GSMA Mobile Privacy Principles to give individuals confidence that their personal data is being properly protected, irrespective of service, device or country[7].

5. United Nations Conference on Trade and Development (UNCTAD), Data Protection Regulations and International Data Flows, 2016.
6. The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy, 2009.
7. GSMA Mobile Privacy Principles: Promoting consumer privacy in the mobile ecosystem, 2011.

Regional data privacy initiatives should be encouraged

The mobile industry believes that individuals around the world have the same concerns over data privacy and security. Where national data privacy regulation is being introduced or updated, it follows that it should be consistent with shared, core principles that apply across a region.

Regional data privacy initiatives such as the APEC Privacy Framework and Cross Border Privacy Rules (CBPR) and the EU's Binding Corporate Rules (BCR) have already moved in this direction, allowing organisations to transfer personal data generally under certain conditions. These frameworks contain accountability mechanisms and are based on internationally accepted data protection principles. However, more needs to be done to make these frameworks more user-friendly for applicants, to encourage other regions to follow suit and, most importantly, to make them interoperable.[8] Interoperability creates greater legal certainty and predictability that allows businesses to build scalable and accountable data protection and privacy frameworks.

Localisation rules risk undermining the protection of personal data

There are several reasons countries seek to impose data localisation rules, including the belief that supervisory authorities can more easily scrutinise data that is stored locally. An additional common reason is the desire to protect individual privacy and ensure it meets the expectations and standards of that country; an obvious way to enforce this is to require that the data stays in the country. However, there are solutions and principles that can mitigate these risks without restricting data flows and the benefits they bring.

Requirements for organisations to use local data storage or technology create unnecessary duplication and cost for companies, and there is little evidence that such policies produce tangible benefits for local economies or improved privacy protection for individuals. Specifically:

- A fragmented approach results in inconsistent protection (e.g., differences across jurisdictions and sectors in what can be stored and for how long) and causes confusion impacting the secure management of personal data.
- Fragmentation through localisation may also create barriers that make investments in security protection prohibitively expensive.
- Collectively, this may undermine efforts by mobile network operators and other service providers to develop privacy-enhancing technologies and services to protect consumers.

8. The common reference model established by a joint APEC / EU working party to drive interoperability between the APEC Cross-Border Privacy Rules (CBPRs) and the EU Binding Corporate Rules (BCRs) is a welcome development

Conclusion

Flows of data across borders are extremely important for societal and economic reasons. Without them, we frustrate not only potential economic growth, but also potential benefits to society of digital transformation. It is therefore incumbent on governments, regulators, industry and civil society groups to reject localisation measures and instead work together to enable the flow of data whilst protecting the personal data and privacy of individuals.

Key Policy Recommendations

- **Facilitate cross-border data flows in a way that is consistent with consumer privacy and local laws by supporting industry best practices and frameworks for the movement of data and working to make these frameworks interoperable.**
- **Ensure that these frameworks have strong accountability mechanisms, and that the authorities can play a role in overseeing/monitoring their implementation.**
- **Only impose measures that restrict cross-border data flows if they are absolutely necessary to achieve a legitimate public policy objective. The application of these measures should be proportionate and not be arbitrary or discriminatory against foreign suppliers or services.**

For more information, visit **gsma.com/mobileprivacy**
Follow GSMA Policy on Twitter at **@GSMAPolicy**

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London, EC4N 8AF,
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601