trade
policy brief

OECD
BETTER POLICIES FOR BETTER LIVES

Trade and Cross-Border Data Flows

October 2018

The ubiquitous exchange of data across borders has given rise to a range of concerns by governments and citizens about some of the effects of so much information being collected, transferred and used across borders, especially when personally identifiable information is involved. Concerns related to privacy and security, amongst others, have led governments to update their data-related regulations, with a growing number of countries conditioning the transfer of data across borders or requiring that data be stored locally.

Regulations restricting data flows can have trade consequences, when, for instance, they affect the movement of data that is critical for the co-ordination of global value chains or for an SME to trade.

Why are countries conditioning the flow of data?

Data come in many shapes and forms, and the reasons for governments to restrict or condition data flows can reflect a number of objectives which can include, in broad terms, the following:

- Much of the debate about data flows revolves around the movement of *personally identifiable information*, which raises concerns about privacy. Privacy means different things to different people, it is therefore no surprise that countries adopt different approaches to privacy protection.
- Other measures conditioning data flows are aimed at meeting different regulatory objectives, such as access to information for audit purposes. In this sense, requirements for data to be stored locally can be seen as the online equivalent of a longstanding practice in the offline world of ensuring that information is available to regulators. Such measures can also be *sector-specific*, reflecting particular regulatory requirements.
- Some types of measures conditioning the flow of data relate to national security, either in terms of protection of information deemed to be sensitive, or the ability of national security services to access and review data. The latter in particular can be very broad in nature, providing wide scope for access to *any form of data*.
- Other reasons for conditioning the flow of data or mandating that it be stored locally can be motivated by the desire to use a pool of data to encourage or help develop domestic capacity in digitally intensive sectors, a kind of digital industrial policy. This can reflect a view that data is a resource that needs to be made available first and foremost to national producers or suppliers. These approaches can be *sector specific or apply to a range of data*.

Ensuring that legitimate policy objectives are met in a way that enables the benefits from trade to be reaped can be a challenge. Thinking this through can benefit from unpacking and mapping the different approaches to data flows; and also from thinking about measures through the lens of the market openness principles.

How do countries approach the cross border elements of data protection?

Three broad approaches to cross-border data flows have emerged.

- Some countries have no restrictions on the movement of data, whether personally identifiable or not. They place the responsibility of respecting and protecting the privacy of the individual on the firm that collects and moves the data.
- Another approach conditions the flow of data by permitting its transfer only to countries that have received an adequacy decision in relation to privacy or in the event that appropriate private sector safeguards are provided. Once these conditions are met, data can be transferred across borders.
- The last type of approach relates to countries which only allow data to be transferred on a case-by-case basis and subject to approval or review by the relevant authorities. Such measures can apply to personal data, or indeed to all types of data.

Data transfers are also addressed in bilateral data protection agreements, largely concerned with personally identifiable data and privacy protection. These arise between countries that have not recognised each other as providing equivalent or adequate protection but they wish to engage in data transfers.

Commitments under trade agreements, whether at the World Trade Organisation (WTO) or under regional trade agreements (RTAs), can also be relevant, both in terms of the impact of such data flow measures on existing commitments, or specific provisions addressing data flows.

Data measures may impact goods, goods with embodied or embedded services and digitally enabled services falling under the General Agreement on Trade in Services (GATS) and the General Agreement on Tariffs and Trade (GATT). Commitments and obligations differ under each agreement; for instance, under GATT rules national treatment is automatically extended, while in the GATS national treatment is a negotiated commitment which differs across country and sector. The GATS provides a specific exception for measures necessary for the protection of privacy (Article XIV), and both the GATT and the GATS contain exceptions for measures that members consider necessary for the protection of their national security.

Explicit provisions addressing data localisation and data flows are starting to emerge in Regional Trade Agreements. The first to include language on data flows was the Korea-US agreement, albeit as a best-endeavour clause. More recently, in the negotiated text of the Comprehensive Progressive Trans-Pacific Partnership (CPTPP) parties committed to protect the free flow of data, including personal information, across borders where it is part of business conduct.

That said, there is no agreement on the extent to which data protection measures, in particular in relation to privacy, fall under the purview of trade agreement. For the EU, the protection of personal data and privacy is a fundamental right and, hence, cannot be subject to trade negotiations.

Moving forward

Reaping the benefits of digital trade requires more international co-operation and dialogue on approaches that ensure the interoperability of differing regulatory regimes and technologies. This may involve going beyond the trade community to dialogue with the privacy community – and also to dialogue within the privacy community towards a shared understanding of the range of approaches needed to protect privacy. Other measures conditioning data flows in the name of national security can pose wider challenges for international interoperability and for dialogue.