

## **PIFS E-commerce Training**

### **Data Disciplines: Cross-Border Data Flows**

#### **Context**

With the modern global economy now more reliant on free flow of data than ever, a key question for regulators is: are there any legitimate purposes for Governments to restrict the flow of data across borders?

Disciplines in recent trade agreements have sought to secure the principle that data should be free to flow across borders. However, in recent years some countries have imposed legal requirements on companies to store data within the country – and in some cases to not allow some data to leave the country. This ‘data localization’ requirements typically relate to the ‘data centres’ where data is physically stored.

Countries that impose such restrictions on free data flow may argue that storing data within their country improves national security or citizen safety (for example, to allow investigators to rapidly access data). On the other hand, data localization requirements are shown to increase the cost of doing business overall, and create unnecessary barriers to e-commerce and efficient data storage.

These issues have found their way to negotiations at the WTO, where countries have pushed prohibitions on data localization, refusing to have any disciplines on data localization and ‘middle grounds’ where data localization can only be required for essential objectives.

The issue of financial services is held out for special treatment, given that the data of personal finances is particularly sensitive. Again, positions on disciplines for financial services remain highly polarised.

#### **Common Approaches**

- Countries that have imposed hard obligations on data localization have – generally – started to soften their position due to the practical difficulty of enforcement. Recent Indonesian and Vietnamese laws are a good example.
- Some countries, such as New Zealand, require businesses to store business records (such as tax records) in local data centres.
- The data localization commitments at the global level are split between China (no disciplines at all so that countries can make their own rules) to USA (a prohibition on requiring data localization) to Singapore (data localization can only be required for a ‘legitimate public policy objective’).

#### **Key Policy Questions**

- Does your country seek to ensure free flow of data across borders through an obligation in trade agreements?
- Are there any current laws that require some data to be stored locally?

- If your country sought data localization obligations, would there be sufficient capacity (data centres etc.) for companies to comply?
- Should certain industry sectors be treated specially such as financial services?

## Additional Resources

UNCTAD Digital Economy Report 2021, with focus on free flow of data for development	<a href="https://unctad.org/webflyer/digital-economy-report-2021">https://unctad.org/webflyer/digital-economy-report-2021</a>
Information Technology & Innovation Foundation, survey of data localization	<a href="https://itif.org/sites/default/files/2021-data-localization.pdf">https://itif.org/sites/default/files/2021-data-localization.pdf</a>
Article from Brookings Institute Report on Data & International Trade	<a href="https://www.brookings.edu/blog/up-front/2020/03/06/data-and-the-transformation-of-international-trade/">https://www.brookings.edu/blog/up-front/2020/03/06/data-and-the-transformation-of-international-trade/</a>
World Economic Forum Report on Cross-Border Data Regulation	<a href="https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf">https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf</a>
Guide to Data Protection – Privacy International	<a href="https://privacyinternational.org/data-protection-guide">https://privacyinternational.org/data-protection-guide</a>

## **PIFS E-commerce Training**

### **Consumer Trust: Online Consumer Protection**

#### **Context**

Should the same protections given to offline consumers be extended to online consumers? If so, what are the additional risks in e-commerce that must be addressed? These are the key question behind the development of 'online consumer protection' rules.

The risks are generally in two areas: (i) the risks relating to not being physically present when making a decision to buy/sell, and (ii) the risks relating to personal data.

On the first risk, rules should give consumers confidence that a seller is not being misleading or deceptive about the products or services, and should have a way to resolve any disputes that later arise.

On the second risk, rules should give consumers confidence that personal data will only be used for the specific purpose of the transaction, and will remain secure.

#### **Common Approaches**

- Rules for Online Consumer Protection in trade agreements are typically about ensuring a framework – for example, rules to require the seller to provide all information necessary for a customer to make an informed decision – including identify of the seller, the quality of the goods/services etc.
- Rules may also extend to hard or soft obligations on the establishment of online/alternative dispute resolution, and rules to prohibit or reduce unsolicited commercial emails (known as 'SPAM')
- Trade Agreements with personal data protection commitments typically require that national laws will obtain consent from consumers for collection and use of their data, and to protect that data from unauthorised use.

#### **Key Policy Questions**

- What flexibility in commitments is needed to ensure you can meet obligations? Should commitments be mandatory? Best endeavours? 'subject to domestic laws'?
- Should a certain international standard form the basis of a commitment?
- What agencies would oversee implementation of commitments? What resources do they have to expand their oversight to e-commerce?
- On consumer protection, is an alternative (or online) dispute resolution mechanism feasible?
- On data protection, should Government be bound by same disciplines?

## Additional Resources

A recent discussion on the growth in generation of data globally	<a href="https://www.idc.com/getdoc.jsp?containerId=prUS47560321">https://www.idc.com/getdoc.jsp?containerId=prUS47560321</a>
UNCTAD's database of online consumer protection laws globally	<a href="https://unctad.org/page/online-consumer-protection-legislation-worldwide">https://unctad.org/page/online-consumer-protection-legislation-worldwide</a>
OECD Recommendations on Consumer Protection in E-commerce	<a href="https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf">https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf</a>
Brief on Online Dispute Resolution	<a href="https://www.oecd.org/digital/consumer/1878940.pdf">https://www.oecd.org/digital/consumer/1878940.pdf</a>
Guide to Data Protection – Privacy International	<a href="https://privacyinternational.org/data-protection-guide">https://privacyinternational.org/data-protection-guide</a>