Australian National University

Data trade and data protection EU and IEAs

Ottavio Quirico

With the support of the Erasmus+ Programme of the European Union

International economic system based on various overlapping flows

Cross-border flow

physical flows via means such as maritime transport

documentary flows

financial flows underpinning transactions between buyers and sellers, via banks

Technologies

Internet of Things (IoT)

Optical Character Recognition (OCR)

Natural Language Processing (NLP)

Privacy and security issues

EC/EU initiatives

2001 European Commission communication on computerised transit procedures
→ aiming to facilitate monitoring and controlling trade in goods

2003 Commission Communication on electronic customs
→ establishing a simplified and paperless environment

2008 E-customs decision
→ establishing the foundations of an interoperable electronic customs environment via a unified data system, simplifying communication between economic operators and customs authorities

2013 Union Customs Code
→ facilitating electronic communications among European customs authorities and between customs authorities and economic operators

2019 EU designed a structured process for the future of customs to 2040

1995 Union Data Protection Directive

2000 EU Charter of Fundamental Rights

Article 8 → data privacy as a fundamental right

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority

EUCFR Article 52(1)

Derogations from the right to personal data protection are only allowed by law subject to proportionality, in the genuine interest of the Union or to protect the rights and freedoms of others

2016 Union Regulation 2016/679 on general data protection (GDPR)

right of access to data
transparency
rectification
erasure
portability (moving data)
objection to automated decision-making
(Articles 5 ff)

Procedure: respect for the right to privacy when data are transferred to a recipient is monitored by a ‘controller’ via a ‘processor’ (Article 2)

Scope of application

Internal market
Situations where EU law applies extraterritorially
Foreign operators who target the EU market by providing goods and services to natural and legal persons within the territory of the Union
Data sent by operators situated in the EU to third countries

Third countries

Few countries have adopted a data protection policy as stringent as that of the EU

Cross-border personal data transfer outside the internal market possible if:

1 The European Commission grants an adequacy decision about the data protection system in a third country (GDPR Article 45): Japan, UK, no EU-US privacy shield (Schrems II)

2 Specific derogations under GDPR Article 49, eg, explicit consent by the data owner
Most countries outside the EU rely on standard contractual clauses as a mechanism for personal data transfer

→ CJEU has clarified in *Schrems II* that standard contractual clauses cannot be considered 'essentially equivalent' to EU data protection in principle, but necessitate a case-by-case assessment, including the possibility for trading companies of adopting 'supplementary measures

EU and international economic agreements

The EU is fostering the adoption of specific regulation related to cross-border data flow via bilateral and multilateral economic agreements, particularly through sections dedicated to digital trade

→ EU-Indonesia Trade Agreement

→ EU-Australia proposal on digital trade

Article 1 (Cross-border data flows)

1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:

(i) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; (ii) requiring the localisation of data in the Party's territory for storage or processing; (iii) prohibiting storage or processing in the territory of the other Party; (iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.

2. The Parties shall keep the implementation of this provision under review and assess its functioning in 3 years following the entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration.

Article 2 (Protection of personal data and privacy)
1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.
2. Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards. 3. Each Party shall inform the other Party about any safeguard it adopts or maintains according to paragraph 2. 4. For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person. 5. For greater certainty, the Investment Court System does not apply to the provisions in Articles 1 and 2.

Article 3 (Cooperation on regulatory issues with regard to digital trade)

1. The parties shall maintain a dialogue on regulatory issues raised by digital trade, which shall inter alia address the following issues: the recognition and facilitation of interoperable cross-border electronic trust and authentication services; the treatment of direct marketing communications; the protection of consumers in the ambit of electronic commerce; and any other issue relevant for the development of digital trade.

2. Such cooperation shall focus on exchange of information on the Parties' respective legislation on these issues as well as on the implementation of such legislation.

3. For greater certainty, this provision shall not apply to a Party's rules and safeguards for the protection of personal data and privacy, including on cross-border data transfers of personal data.

EU regime protecting personal data, particularly under the GDPR, quite restrictive of international cross-border data trade, requiring States outside the EU to improve their level of protection

→ limiting investment and trade that are based on data transfer

Data trade is governed by the discipline of services

→ Personal cross-border data restrictions are allowed under general international law: there are no obligations to ensure free trade in services

→ EU data protection regulation should be considered customarily allowed

WTO: according to the 1995 General Agreement on Trade in Services (GATS) cross-border data trade must be in principle free, based on the most-favoured-nation (MFN) and national treatment (NT) principles.

→ Accepting the conditions established by the EU for data flowing from the Union might create a disparity with respect to local data flows in a non-EU country (NT)

→ Acknowledging data trade with third countries based on adequacy decisions might not be fully consistent with the MFN principle

GATS: asymmetric restrictions to services might be justified based on the regime of general exclusions under Article XIV

Premise → lawfulness of derogatory measures subject to the requirement that they are not a means of arbitrary or unjustifiable discrimination between countries where like conditions apply, or a disguised restriction on service trade

Article XIV(c)(iii) → necessary measures concerning 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data' as well as 'the protection of confidentiality of individual records and accounts'

Is the EU personal data protection system restricting international trade consistent with the 'necessity' test
→ least restrictive of international trade to fulfil the right to privacy? (WTO DSU)

Less restrictive data trade regimes (than EU) actually exist in the world

Rationale underpinning the EU approach → adopting the least restrictive regulatory framework for the right to privacy according to the EUCFR, in compliance with EU data protection and privacy rules

Rationale of the GATS → adopting the least restrictive barriers to cross-border data flows

The EU restrictive regime protects the first data transfer to a third country (A), but the further transfer of data from State (B) to another State (C) is unlikely to be afforded equivalent protection

(unless MFN clause is added to horizontal clauses on data transfer in a treaty between the EU and a third State (B))

Test of necessity has been elaborated by the WTO jurisdictional bodies as concerns trade in goods and services, but not particularly with respect to data trade

→ possible that the test of necessity for data trade needs to be assessed differently from other forms of trade

Practice will clarify the issues

→ compelling a general improvement of privacy in cross-border data flows; or

→ lowering data protection requirements in EU cross-border transactions