



DATA FLOWS AND TRADE AGREEMENTS

BRIEFING TO DEPARTMENT FOR INTERNATIONAL TRADE

1 Risks to adequacy systems and data protection in UK-Japan and CPTPP

1.1 In this note we set out the work of leading trade academics that have set out the risks to “data adequacy” systems for data flows, set out in the Data Protection Act 2018, in agreements such as the UK Japan CEPA and the CPTPP which seek to liberalise cross-border data flows.

1.2 The Department for International Trade has not as yet acknowledged the risks from data flow clauses in these agreements,¹ going as far as to dismiss them in a public document on the UK Japan CEPA.² However, the European Union, under advice from academics and civil society, has taken the opposite view in its trade negotiations, in order to safeguard GDPR provisions against potential legal challenges under the WTO GATS Article XIV. As a result, the EU has negotiated language in treaties to safeguard their right to legislate their data protection regime, and have not agreed language on data flows similar to that contained in CPTPP.

1.3 The potential for conflict between data protection and trade law dates back to WTO GATS, but has been discussed concretely since 2017. Where the EU has taken steps to minimise the risks to privacy and other fundamental rights from trade deals, the UK - in contrast - is pushing the limits of what may be legally acceptable. In particular, there are risks that the UK’s own Adequacy system set out in the DPA 2018³ could be challenged as disproportionate, either under WTO GATS, or under the ‘four step test’ contained in CPTPP for restrictions to data flows. The UK needs to ensure these risks are eliminated or at least mitigated.

1.4 The ability of the UK to conclude its own “data adequacy” agreements with other countries is a powerful mean to liberalise data flows while ensuring that privacy and data protection rights remain enforceable. It is a sustainable approach to international trade.

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929181/CS_Japan_1.2020_UK_Japan_Agreement_Comprehensive_Economic_Partnership_v1.pdf Article 8.80 and 8.84 in particular; and <https://www.dfat.gov.au/sites/default/files/14-electronic-commerce.pdf> Article 14.11 TPP, incorporated by CPTPP

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/941402/uk-japan-cepa-data-protection-explainer.pdf

3 <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/>

Moving away from it would create business uncertainty and costs, and undermine data adequacy with the EU. Thus the ability of another country to challenge the UK's right to operate an adequacy system must be carefully analysed and understood.

1.5 We draw particular attention to the work of Kristina Irion from the University of Amsterdam and Graham Greenleaf from the University of New South Wales. Many other academics have drawn similar conclusions.

2 Summary of the main concerns

2.1 The EU model of data protection currently in place in the UK is already at risk under WTO regulations and digital trade liberalisation increases this risk.

2.2 The EU has sought to minimise this risk by incorporating standard horizontal clauses in its trade agreements⁴ that would prevent other parties from challenging the EU regime. Data flows are to be regulated through adequacy decisions as prescribed by the DPA 2018 and not trade deals.

2.3 The UK has taken a completely different approach, incorporating the text of the CPTPP and US agreements in the UK Japan CEPA and trying to join the CPTPP. As the legal risks depend on the motivations of the countries, the risks increase as the UK's agreements involve more countries, or interact with agreements those countries have made that may oblige them to seek looser protections.

2.4 DiT needs to explain why it believes that the UK does not face the same legal risks as the EU is seeking to minimise and therefore is able to take a different approach.

2.5 These risks are particularly acute if the UK joins the CPTPP, as this treaty has been identified as driving lower privacy standards.

2.6 DiT needs to examine its commitments that the UK has signed with Japan, and would sign with the CPTPP and other agreements, to ascertain whether these are compatible with the UK GDPR regime without any changes or special arrangements;

2.7 If DiT finds that there are legal risks to UK GDPR, it will need to adjust its position to ensure that UK GDPR cannot be challenged, by means of additional measures such as a 'side note' to any agreement to establish that parties will not challenge UK GDPR and the UK adequacy system for data flows.

3 General risks to the UK data protection from trade

3.1 Dr Kristina Irion is Assistant Professor at the Institute for Information Law (IViR) at the University of Amsterdam. She is a leading European expert on the interaction of EU data protection law and trade.

3.2 Dr Irion's work has been instrumental in providing the evidence which helped shape the current EU position towards data in trade agreements. Her 2016 report on Trade and Privacy identified the risks to the regulatory autonomy of the EU from digital trade.⁵ The report was commissioned by NGOs, and found that the EU data regime had strong safeguards against "involuntary liberalisation via the international trade agreements to

4 With the exception of the EU UK Trade and Cooperation Agreement, which contains a modified version deemed problematic by EU consumer groups.

5 Irion, Kristina and Yakovleva, Svetlana and Bartl, Marija, Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements (July 13, 2016). Available at SSRN: <https://ssrn.com/abstract=2877166> or <http://dx.doi.org/10.2139/ssrn.2877166>

which the EU is party". However, there are enough residual risks of inconsistency with WTO law and the public policy exceptions to require specific safeguards, such as the EU horizontal model clauses.

"This (EU) carve-out primarily takes the form of a broad exception for domestic privacy and personal data protection rules, which (...) explicitly states that any rules for cross-border transfers of personal data constitute a priori appropriate measures and recognizes that the protection of privacy and personal data is a fundamental right."⁶

"To date no case law has clarified the application of (WTO GATS) Article XIV(c)(ii) to privacy and personal data protection measures. Scholars and pundits note a high level of uncertainty and unpredictability in relation to the application and interpretation of the general exceptions."⁷

3.3 Dr Irion has engaged with several of the best known concerns about the potential conflicts between European data protection and trade law, rejecting some of these claims, e.g. that restrictions could amount to a 'zero quota' market access, or that negative adequacy decisions could be discriminatory. Nevertheless she found that the EU adequacy regime was open to challenge of discrimination due to the lack of structured processes and political influence.⁸ Besides, there are necessity and proportionality risks:

"The 'necessity' of these (GDPR) rules could be successfully challenged if the complaining party invokes that there are less restrictive alternatives, such as the principle of accountability, adopted in Canada and many Asia-Pacific Economic Community countries."⁹

3.4 Other scholars have also argued that "alternatives" to GDPR mechanisms could be put forward, such as end to end encryption, consent or remedial measures.¹⁰

3.5 Dr Irion stresses that it is unlikely that a country would take on the EU, but this case is less clear with the smaller UK.

4 Specific issues with the CPTPP and Japan

4.1 The UK and EU have granted Japan adequacy, and on the surface this may appear to show that the clauses in the Japan-UK CEPA are compatible with current data protection adequacy systems. However, these clauses have not been used aggressively in a trade

6 Yakovleva, S., & Irion, K. (2020). Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation. *AJIL Unbound*, 114, 10-14. doi:10.1017/aju.2019.81

7 Yakovleva, Svetlana and Irion, Kristina, The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection (November 29, 2016). S. Yakovleva and K. Irion, "The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection," (2016) European Data Protection Law Review 2(2): 191-208, Amsterdam Law School Research Paper No. 2016-65, Institute for Information Law Research Paper No. 2016-05, Available at SSRN: <https://ssrn.com/abstract=2877168>

8 ibid.

9 ibid.

10 Andrew D. Mitchell & Jarrod Hepburn, DON'T FENCE ME IN: REFORMING TRADE AND INVESTMENT LAW TO BETTER FACILITATE CROSS-BORDER DATA TRANSFER, 19Yale J.L. & Tech(2018). Available at: <https://digitalcommons.law.yale.edu/yjolt/vol19/iss1/4>

dispute. It may be that Japan would not seek to do so, thus the Japan agreement may in practice pose a low threat. Even so, Japan's trade agreement with the USA, which precedes the UK's agreement, commits Japan to ensure easier data flows, and thus may conflict with its adequacy arrangements and treaty with the UK, so could be open for the USA to place pressure on Japan to seek more flexible data flow arrangements with the UK.

4.2 Each agreement struck can be viewed as a risk, and the UK needs to seek to ensure it is not under legal threat, assuming that the UK does indeed intend to operate a system of granting adequacy to specific countries to ensure easy data flows. CPTPP poses a greater threat as many more countries are signatories, it includes some opportunities for ISDS to be employed, and the USA may seek to join. Many of those countries with lower data protection standards may seek to push the UK to accept more permissive standards for data flows.

4.2 Professor Graham Greenleaf from the University of New South Wales is one of the best known experts in data protection in the Asia Pacific region, having written the ground-breaking monograph *Asian Data Privacy Laws: Trade & Human Rights Perspectives*.¹¹ Professor Greenleaf has raised extensive concerns about the negative impacts that CPTPP could have on data protection.

"Any exceptions from this obligation (on data flows in CPTPP) must be justified under the 'four step test' which requires a restrictive measure to satisfy four requirements..."

In earlier FTAs, States have not had the onus of proving all four such requirements. This version may impose a 'regulatory chill' on governments considering stronger data export limitations, particularly when coupled with ISDS provisions...

These CPTPP requirements still embody the type of binding international privacy treaty that those opposed to data privacy would like to achieve: (a) no substantive or meaningful requirements to protect privacy; (b) coupled with prohibitions on data export limitations or data localisation requirements that can only be overcome by a complex 'four-step test' of justification...¹²

4.2 Article 14.11(3) of the treaty sets out a narrow 'four-step test' for public interest measures to restrict cross-border data-flows:

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

*(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
(b) does not impose restrictions on transfers of information greater than are required to achieve the objective*

11 Greenleaf, Graham (2017). *Asian data privacy laws: Trade and human rights perspectives*. Oxford: Oxford University Press.

12 Greenleaf, Graham, Looming Free Trade Agreements Pose Threats to Privacy (April 3, 2018). (2018) 152 Privacy Laws & Business International Report, 23-27, UNSW Law Research Paper No. 18-38, Available at SSRN: <https://ssrn.com/abstract=3199889>

4.3 This test aims to stop participating governments creating unfair advantages for their companies under the guise of protecting some higher values, but in practice it sets a high bar that can be used to restrict legitimate policies. A “legitimate public policy objective”, such as protecting privacy and data, cannot be “arbitrary or unjustifiable” or a “disguised restriction on trade”. It must restrict data flows only enough “to achieve the objective”, and no further.

4.4 The question is open therefore as to whether the UK’s “adequacy decisions” are “arbitrary”, a “disguised restriction on trade”, and whether the same policy objective could be achieved by a less restrictive measure. Similarly to the WTO, if challenged under CPTPP, the UK may have to show that it has no alternative mechanisms available for cross border transfers. This may be hard to argue in a context where most other countries use less restrictive measures that are explicitly accepted as valid in the text of the treaty. As explained by Dr Mira Burri from the University of Lucerne:

“A commitment to lower standards of protection is particularly palpable in the field of privacy and data protection... TPP Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent.”¹³

4.5 In addition, the same charges of arbitrariness and discrimination discussed by Dr Irion in relation to the EU and the WTO could also be levelled here against the UK if it enables unrestricted data flows to certain CPTPP countries under adequacy – currently only Japan and New Zealand - and not the rest.

4.7 If the UK ends up following the CPTPP exception regime this could affect its own adequacy decision from the EU:

“(...) it is not certain that the CPTPP’s “four step test” for data export restrictions is consistent with the GDPR’s requirements for adequacy, particularly in light of the Schrems II decision of the CJEU”¹⁴

4.8 In the Schrems II case, the Court of Justice of the EU invalidated the main data transfer mechanism used by large companies to send data from the EU to the US, called Privacy Shield. The ruling has brought into focus that in the EU data regime respect to fundamental rights, such as privacy and due process, is paramount. The European system could almost be described as the complete inverse of the CPTPP. While in the Asia Pacific regime, any interference with businesses ability to transfer data must meet the ‘four step test’, in the EU any interference with fundamental rights, such as putting personal data at risk through transfers outside the EU, must pass its own test.

13 Burri, Mira, The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation (November 9, 2017). UC Davis Law Review, Vol. 51, 2017, pp. 65-133, Available at SSRN: <https://ssrn.com/abstract=3067973>

14 Privacy laws & Business International Report, October 2020,
<https://www.privacylaws.com/reports-gateway/reports/>

4.9 The ISDS provisions in CPTPP increase the risks to the UK data protection framework because while states may have wider considerations, companies will focus on their own priorities.

"The most significant investment protection relevant to data privacy (in ISDS in CPTPP) is the prohibition of direct or indirect expropriation of investments, except for a public purpose and for payment of fair and prompt compensation (art. 9.7.1). Failure to compensate will lead to the threat of ISDS procedures. While a breach by a party of the data export limitation or data localisation provisions will not automatically trigger entitlement to ISDS provisions by affected companies (art. 9.6.3). It could, if such breaches can be said to constitute an indirect expropriation of the investment in a company (for example, one established to be dependent on information surveillance). If so, then the possibilities of ISDS actions should frighten any country that has a data privacy law but has a smaller litigation budget than an Internet giant based in another party. Perhaps Google or Facebook are for the moment based in the wrong country, but will that change? Countries may need to draw breath both before enacting new laws, and before embarking on any strong enforcement of existing laws, for fear of an ISDS reaction. So, although ISDS provisions do not affect privacy per se, their interaction with data export or data localisation provisions could do so, and quite severely."¹⁵

5 Conclusion

5.1 We have taken the step of sending this short note with the hope that it will help improve the engagement of the Department of Digital Trade with civil society and business over the substantial risks that the Asia Pacific pivot of digital trade brings to British data protection. The quotes and references we present show that the concerns are serious challenges shared by world class legal experts that require serious consideration. We are looking forward to continuing these discussions.

5.2 If the UK continues to pursue membership of the CPTPP it must consider what safeguards may be available to ensure that the domestic data protection regime is protected from "involuntary liberalisation" that may impact the rights of people in this country. One possible solution might be to make membership conditional on the other countries agreeing to a side letter that excludes the UK from the commitments on data. This could include language similar to the EU's horizontal clauses. Alternatively, Article DIGIT.7 *Protection of personal data and privacy* of the EU-UK Trade and Cooperation Agreement, appears to be designed to protect the regulatory autonomy of the UK in this respect. As such, it may be a candidate for inclusion in any side letters or alternative arrangements. However, this text is untested and it may not provide sufficiently robust safeguards. In particular the requirement to provide for 'instruments enabling transfers under conditions of general application for the protection of the data transferred' needs to be explained by the government in detail.

15 Ibid. note 11