A Tale of Two Data Regimes: Can the EU-Japan Adequacy Decision be challenged?

15 February 2023

Hiroshi Miyashita
Professor of Law, Chuo University
Global Context of the Japan’s data flow

- **EU**: Mutual Adequacy Decision
- **OECD**: Member of GPEN and OECD Privacy Guidelines
- **GPA**: Member of Global Privacy Assembly
- **G7**: Member of G7 Data Protection and Privacy Authorities
- **APPA**: Member of Asia Pacific Privacy Authorities

### Council of Europe
- Observer for Convention 108+
- Member of Cybercrime Convention

### APEC
- Member of APEC Cross-Border Privacy Rules (CBPRs)

### 21 Trade Agreements
- Singapore, Mexico, Malaysia, Chile, Thailand, Indonesia, Brunei, ASEAN, the Philippines, Switzerland, Viet Nam, India, Peru, Australia, Mongolia, the Trans-Pacific Partnership (TPP)12 (signed), the TPP11, the EU, the US, the UK (signed), the Regional Comprehensive Economic Partnership Agreement (RCEP) (signed)
PPC’s Survey on Data Transfer

Third Countries of Exporting Personal Data from Japan

- US: 158
- China: 55
- Singapore: 42
- Germany: 37
- UK: 34
- Thailand: 30
- Vietnam: 28
- South Korea: 24
- Taiwan: 23
- Indonesia: 22
The Commission considers that the APPI (the Japanese Act on the Protection of Personal Information) as complemented by the Supplementary Rules contained in Annex I, together with the official representations, assurances and commitments contained in Annex II, ensure a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679. (para 171)

this Decision should be subject to a first review within two years after its entry into force (para 181)

“This adequacy decision creates the world’s largest area of safe data flows. Europeans' data will benefit from high privacy standards when their data is transferred to Japan. Our companies will also benefit from a privileged access to a 127 million consumers' market. Investing in privacy pays off; this arrangement will serve as an example for future partnerships in this key area and help setting global standards.”
-Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, 23 January 2019
Adequacy process for Japan

Joint declaration & statements

- Joint declaration by Mr. Shinzo Abe, Prime Minister of Japan and Mr. Jean-Claude Juncker, President of the European Commission, 6 July 2017
- Joint statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, 14 December 2017
- Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, 31 May 2018
- Joint Press Conference by H.E. Mr. Shinzo Abe, Prime Minister of Japan, H.E. Mr. Donald Tusk, President of the European Council, and H.E. Mr. Jean-Claude Juncker, President of the European Commission, Following the Signing of the Japan-European Union Economic Partnership Agreement and Japan-European Union Strategic Partnership Agreement, 17 July 2018
- Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, 17 July 2018
2019 Adequacy decision

- Rikunabi case
  - HR platform sold recruiting personal data (26,060) without consent
  - PPC’s recommendations

EDPB’s opinion
EP’ resolution

2019

2020 APPI Amendments
- 3 year review
- Prohibition of improper utilization
- Introducing pseudonymously processing information
- Abolishing short-term data
- Mandatory data breach notification
- Penalties lifted up to 100 million yen

LINE scandal
- Allowing SNS data (86 million users) to access by the Chinese companies and transfer some data to Korea
- PPC’s instruction

2020

2019

2021

2021 APPI Amendments
- A part of Digital Reform Laws
- Integrating public/private sectors into APPI
- PPC’s powers into the public sector
- Setting Common rules such as definition for local ordinances
- Restricting research purpose exemption

2021 Amendments

Rikunabi case
- HR platform sold recruiting personal data (26,060) without consent
- PPC’s recommendations

Enforcement by the PPC

- No enforcement actions regarding the data transfer from the EU
- Administrative instruction against LINE for data scandal
- First criminal sanction initiated by the PPC on the bankrupters’ mapping case

---

Chapter 5
A Tale of Two Privacies: Enforcing Privacy with Hard Power and Soft Power in Japan

Hiroshi Miyashita

The ICO’s courageous decision may be regarded as hard power entailing a legal sanction in order to change the corporation’s behaviour. In contrast, the Japanese approach indicates soft power by social and cultural enforcement in order to rebuild trust with customers. In London, the monetary penalty sought to address the damage and distress of data subjects. Under the British approach, a fine may be more effective in altering the corporate mentality and deterring future security breaches, whereas in Tokyo, the public apologies and voluntary compensation went some way to regaining public trust and rebuilding a close relationship with customers. In the Japanese business climate, the risk of reputational damage and loss of customer trust may be more serious for corporations than paying fines in data breach cases.
Data Transfer Rules under the APPI

1. Consent
   - Consent by data subjects
   - Information to be provided (the name of the third county, personal information protection system, the measures taken by the recipient party)

2. A protection system conforming the PPC’s Rule
   1) Obligations under the APPI in a proper and reasonable way (MoU, contracts) – with references to the OECD Privacy Guidelines and the APEC Privacy Framework
   2) Certification- APEC CBPR System (only 3 companies as of February 2022)

3. Equivalency decision by the PPC
   - 31 EEA + the UK

... the requirements set forth in Supplementary Rule (4) exclude the use of transfer instruments that do no create a binding relationship between the Japanese data exporter and the third country's data importer of the data and that do not guarantee the required level of protection. This will be the case, for instance, of the APEC Cross Border Privacy Rules (CBPR) System, of which Japan is a participating economy, as in that system the protections do not result from an arrangement binding the exporter and the importer in the context of their bilateral relationship and are clearly of a lower level than the one guaranteed by the combination of the APPI and the Supplementary Rules. (para79)
Chapter 8  Trade in Services, Investment Liberalisation and Electronic Commerce

Article 8.3 General exceptions

Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or trade in services, nothing in Sections B to F shall be construed as preventing a Party from adopting or enforcing measures which are:

(c) **necessary to secure compliance with laws or regulations** which are not inconsistent with the provisions of this Chapter including those relating to

(ii) **the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts**;

On 21 December 2018, in Brussels (Belgium), Japan and the European Union exchanged diplomatic noted to notify each other that their respective applicable legal requirements and procedures for entry into force of the Agreement between the European Union and Japan for an Economic Partnership (Japan-EU EPA) have been completed. With this exchange of notes, the Agreement entered into force on 1 February, 2019.
ARTICLE 8.73 Source code
1. A Party shall not require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

Trade Agreement between Japan and the United States of America concerning Digital Trade (entry into force on 1 January 2020)
ARTICLE 17 Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory.

Cf.) EU-UK Trade and Cooperation Agreement Article DIGIT.12: Transfer of or access to source code
1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party
ARTICLE 22 Automated individual decision-making, including profiling
1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or
   (c) is based on the data subject’s explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

ARTICLE 13 Information to be provided where personal data are collected from the data subject
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
   (d) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

"Controllers cannot rely on the protection of their trade secrets as an excuse to deny access or refuse to provide information to the data subject."
Speeches from Chancellor Merkel and Prime Minister Abe on 23 January 2019 at the World Economic Forum
DFFT (Data Free Flow with Trust)

- The Prime Minister’s Speech at the World Economic Forum (January 2019)
  ‘Let Osaka G20 set in train a new track for looking at data governance--call it the Osaka Track--under the roof of the WTO.

  We have yet to catch up with the new reality, in which data drives everything, where the D.F.F.T., the Data Free Flow with Trust, should top the agenda in our new economy.

- G20 OSAKA LEADERS’ DECLARATION (June 2019)
  ‘... we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow with trust will harness the opportunities of the digital economy.’

- Japan’s host of the G7 Summit in 2023
  OECD Declaration on Government Access to Personal Data Held by Private Sector Entities
  Digital Minister: New international body with permanent secretariat
  PPC Global Strategy: global corporate certification system

WTO and Data Flow Rules

- General Exemption clause (GATS Art.14(c)(ii)) of ‘the protection of the privacy of individuals in relation to the processing of dissemination of personal data’ and ‘a means of arbitrary or unjustifiable discrimination’

- ‘The WTO has many Members, so providing it with rules on digital trade that materialize "Data Free Flow with Trust" (DFF) will make business more predictable and stable. This will in turn promote further digital trade. With the aim of achieving early results, we will work to accelerate and add further impetus to the negotiations’
A Tale of Two Data Regimes: Can the EU-Japan Adequacy Decision be challenged?

15 February 2023

Hiroshi Miyashita
Professor of Law, Chuo University