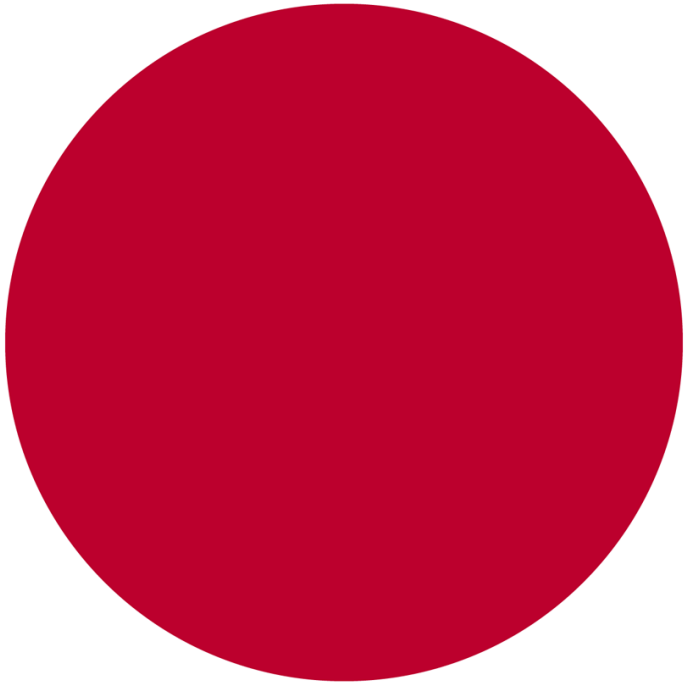
JAPAN



[ADPL Ch 8 ‘Japan – The Illusion of Protection’]

Japan

- Privacy rights outside PPIA
  - Implied constitutional protection of privacy under A 13; never yet breached!
  - Civil CodeL some negligent disclosure and 'right to forget' cases
- Complexity of the main legislative structure (2003-)
  - *Protection of Personal Information Act 2003* (PPIA) covers both private sector (principles and enforcement) & public sector (principles only)
    - 4 other Acts cover enforcement in the public sector etc
  - The *'Basic Policy'* and the *Cabinet Order* on enforcement (both rev 2008) are relevant to all
  - 38 (non-binding) *Guidelines* for the private sector(s) set by each Ministry
    - Rationalisation based on METI Guidelines (rev 2009)
  - 1799 municipal *Ordinances* on data protection
- 2015 PPIA Amendments – see *2017 Update* pp 24-25
  - Major changes, closer to international standards
  - Created a DPA (PIPC) for 1st time, with independent status
  - Only in effect since May 2017: no track record yet

Japan – Privacy Principles (post-2017)

2019 update p.8

- **Access and correction** rights are now explicit
- **Deletion** requirement for the first time
- **Disclosure** limitation is **undermined** by ability to merely publish on a website (non-identified) details of intended disclosures and invite opt-outs (A 23(2));
  - Notice also required to PIPC , who must also publish it
- **Collection** is **not explicitly limited** to what is necessary for the specified purpose (A 17)
- **Data export limitations**, with PIPC to decide Whitelist; PIPC can allow exports to APEC CBPRs compliant companies (the 'Japanese back door') [But not from EU-sourced data]
- Some notification of data breaches (**DBN**) required
- Many weaknesses remain, compared with EU: 2019 update, p.8

Result: *Japan's principles were OECD basics or less; now closer to Asian average of 5/10 'European' principles*

Japan – (non)Enforcement (pre-2017)

- No basis for damages claims before Courts (or anyone else)
  - No provisions in Act for payment of compensation
  - Breach of PPIA does not give civil damages claim (2007 Tokyo District Court)
  - 2018 *Benesse* decision that birthdates of 35M children was 'not private enough'
- Investigation of complaints under PPIA (pre-2017)
  - Complaints may be filed with 4 types of bodies: (i) the business; (ii) 39 APIPOs (sectoral business bodies); (iii) local government; or (iv) National Consumer Affairs Centre – BUT not the relevant Ministry (which has enforcement power). But PPIA set out no procedures.
  - Only published outcomes are for 13 complaints to the National Consumer Affairs body from 2004-07: they explain nothing
  - No evidence of any outcomes by other mediation
  - The complaints system had zero transparency
- Enforcement by Ministries
  - Ministries cannot issue fines; they could collect reports (often); make recommendations (7 in 7 years); and issue compliance orders (ø in 7 years) – so there were ø prosecutions for non-compliance.

Bottom line = no evidence of enforcement Question: Has anything changed?

Japan – Enforcement? (post-2017)

- Personal Information Protection Commission (PIPC) [from 2017]
  - Previous ‘Ministry-based’ system replaced by PIPC as a DPA for the private sector
  - Ministry of Internal Affairs (MIC) is DPA for public sector
- PIPC (9 Commissioners) has strong legal independence
- PIPC Rules implement Act & Cabinet Order (delegated legislation)
- PIPC powers
  - strong powers to investigate, find breaches, and give advice/recommendations/orders
  - No PIPC administrative penalty (except US$3K for disobeying PIPC orders)
  - Fines following prosecutions are trivial (US $10K)
- Still no powers to obtain compensation from courts or from PIPC

Japan – Enforcement? (post-2017) (cont.)

Will PIPC use powers? (Ministries did not pre-2017)

- PIPC website (English version) gives zero information on enforcement actions since 2017
- PIPC website (Japanese version), gives little more
  - 2018 Annual Report, lists '238 instructions and advice' and 31 mediations, but no details of any;
  - Prof Miyashita finds only 3 cases, all in 2019, where PIPC issued 'recommendations with administrative instructions' (no penalties): *Rikunabi Recruitment Agency* case; *Japan Taxi* case; and *Amazon Japan data breach* case
- Conclusion: Evidence is still absent of any significant *enforcement* of Japan's law
  - various Japanese experts criticise lack of transparency

Japan – Legalising 'Big Data'

- See 2017 update p.25; 2019 Update p.8; 2015 article
- 'Anonymous processed information' (API) – PPIA *requires PIPC to specify de-ID procedures* which may be impossible – uncertainties
  - But *API status results from following procedures*, not from achieving making re-identification impossible
- Bulk API then becomes able to be disclosed/sold to others, but both discloser and recipient still have significant security and publicity obligations
- Is there be a business case for use of API?
  - Report by PIPC on API (Feb. 2017)
  - Extent of use of these procedures is unknown
- API procedures do not apply to data originating from EU
  - Excluded under 'Supplementary Rules', to obtain EU adequacy

Japan – EU adequacy status

- See 2018 Update pp. 6-7; 2019 Update pp. 9-10
- EU Commission Decision held Japan's private sector laws '**adequate**' under art. 45 of the GDPR (Jan. 2019): unrestricted transfer of personal data from EU to Japan
  - European Data Protection Board (EDPB) and EU Parliament (via LIBE Committee) neither endorsed nor rejected the EU COM decision.
- In order to obtain adequacy, Japan's PIPC issued 'Supplementary Rules' **applying *only* to EU-sourced data**:
  1. Additional 'special categories' (sensitive data).
  2. Preservation of protections with no time limits.
  3. Preventing adding disclosures simply by website notice
  4. Requiring that API be 'irreversible for anyone' (ie objective)
  5. Onward transfers to US companies based solely on APEC-CBPRs certification (the 'Japanese back door' is blocked – replaced with a consent requirement

Japan – EU adequacy status (2)

- Main grounds for criticising COM's Japan decision:
  1. Can an 'essentially equivalent' law exclude Japanese citizens?
  2. Still no evidence of enforcement; How is Japan's enforcement regime 'essentially equivalent' to GDPR?
  3. Is consent a sufficient basis for an onward transfer regime?
  4. How significant are other gaps between Japan and EU?
     - automated decisions; design & default; DBN; data portability
     - how important are these to adequacy? ('essentially equivalent')
  5. Limits on public sector access to private sector data? (vital in *Schrems case*) might not be strong enough
     - Annexures to Decision, signed by Japan, purport to limit this
  6. 'Readily collated' requirement in Japan's definition of PI
     - will some EU personal data not be protected? (not raised)

Japan – EU adequacy status (3)

- Result
  - Only CJEU can reverse COM decisions (as occurred under the Directive with EU-US 'Safe Harbor' *Schrems Case*)
    - eg if NOYB NGO (Schrems) challenged a transfer to Japan
  - But EDPB pushed COM to agree to review the decision in 2 years, not 4: pressure on Japan?
  - Decision is vital to the future credibility of adequacy
  - Will other countries say 'I'll have what Japan had'?

Japan – competition law

- Japan Fair Trade Commission (Aug 2019)
  - DRAFT ‘Guidelines Concerning Abuse of a Superior Bargaining Position under the Antimonopoly Act on the Transactions between Digital Platform Operators and Consumer that Provide Personal Information’
  - Guidelines set out what JFTC considers equals abuse of monopoly position in collection and use of PI. When finalised, enforcement actions are possible.
  - Other competition regulators (eg Australia’s ACCC) are investigating competition implications of data privacy abuses

Japan – competition law (cont.)

Conduct = abuse of superior bargaining position

1. Acquiring PI without stating the purpose of use
   - Must give understandable notice of purpose
2. Acquiring or using PI beyond the scope necessary to achieve the purpose of use
   - Must indicate if not necessary and give options
3. Acquiring or using PI without taking appropriate security precautions
   - Low risk if follow PIPC guidelines
4. Acquiring additional information (eg web browsing data) without providing additional services to consumers
5. Provision of PI to 3rd parties without consent