Feb 2020

International: Issues around 'adequate or equivalent protection' in cross-border data transfers and four key steps to take

The proliferation of cross-border data transfers as a common business practice has been accompanied by an increasingly complex legal and regulatory landscape that governs the same. Jeffrey Lim, Director at Joyce A. Tan & Partners LLC, discusses some of these challenges and provides a four-step approach to help firms ensure their compliance when transferring data to parties in other jurisdictions.

imaginima / Signature collection / istockphoto.com

Introduction

A client asks: "Can my Singapore office transfer the personal data overseas?"

The (unnamed) Singapore data protection lawyer responds: "Well, only if you ensure this data receives a *standard of protection that is comparable* to that under Singapore law." He enunciates the italicised words because he's paraphrasing the Singapore Personal Data Protection Act 2012 (No. 26 of 2012) ('PDPA').

So, naturally, the clients asks: "But aren't all data privacy laws roughly the same?"

To which the lawyer says: "Well, that's a *difficult question.*"

And the client protests: "You just want to charge me more money. *Don't* you?"

But it is a difficult question. And no, it is not an excuse to inflate an invoice.

With more and more businesses operating in multiple territories and adopting cloud-based solutions, the use of cross-border transfers of data is increasing. As such, circumventing cross-border data transfer restrictions under data protection or privacy laws has become a necessity.

It can be a question of how different legal systems operate but, in most jurisdictions, cross-border data transfer restrictions mean ensuring that the place where you send your data (the destination jurisdiction) provides an 'adequate level' of protection.

What is adequate, however, can vary. This is where the devil can so often be in the details (or, alternatively, in the invoice rendered).

Adequacy - as determined by public decisions

One way in which adequacy is addressed is through an assessment done via regulatory bodies, the most well-known example of this being the framework of adequacy decisions made by the European Commission ('EC') under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR').

Under this process, a proposal is made by the EC to consider if a particular non-EU jurisdiction meets the adequacy requirements of the GDPR. This is followed by the issuance of an opinion by the European Data Protection Board, which in turn is followed by the consideration (and possibly approval) of the representatives of the EU countries. This process then culminates in the adoption of the decision of the EC[1].

When a positive adequacy decision is issued for a particular jurisdiction, the EC is essentially 'whitelisting' that jurisdiction, i.e. determining it as having adequate levels of protection for personal data such that the transfer of personal data from inside the EU to that country does not need any further authorisation.

A comparative review of the analytical steps used in the adequacy decisions issued so far would make for an interesting article in itself, but for this article, it is enough to peek into a recent adequacy decision, namely that in respect of Japan (23 January 2019)[2].

In this instance, the analysis goes into a summary and review of the Japanese data protection laws such as the Act on the Protection of Personal Information ('Act No. 57 of 2003') ('APPI') including:

- a review of concepts under the APPI;
- rights, obligations, exclusions, and other safeguards under the APPI;
- oversight and enforcement, touching on powers of enforcement and judicial redress; and
- a review of the impact of that country's law on public authorities and their ability to be checked/limited in their access to that data (an important topic in the wake of the *Schrems*[3] case).

Notably, there is no mention of statistics or any analysis on the costs of enforcement, nor any discussion as to difficulties or ease of access to justice. In other words, the analysis does not go into what a layperson might consider 'real-world considerations.' As practical 'on-the-ground' issues in getting redress are difficult to quantify and assess however, this is understandable.

To businesses, this process is beneficial for the clarity it provides. However, as with many governmental processes, it can take time. The process has been in existence since the 1990s but, as at the writing of this article, only a dozen jurisdictions have received a positive adequacy decision and Japan is only the second jurisdiction in the Asia Pacific region to be given such a decision.

Adequacy - as achieved by private agreements/arrangements

Given the practical need to get on with business quickly and efficiently, this issue of speed makes it necessary to also consider reliance on private agreements (e.g. bilateral/multiparty contracts) and arrangements (such as policies, processes, and audits).

Private agreements and arrangements ultimately place the focus on the individual party (or parties) and the private steps they personally take to ensure that the transfer of data out of the country meets standards. In the context of the GDPR, data transfer tools include the use of Binding Corporate Rules ('BCRs')[4], consent arrangements, and data transfer agreements using model terms.

From a legislative perspective, this approach usually includes multiple facets involving an assessment of the viability of the safeguards implemented in each case.

This approach does not mean that the actual legislative or regulatory status of the destination jurisdiction is rendered irrelevant but the focus instead shifts to individual arrangements as means of achieving compliance.

Of course, the divide between public and private arrangements is not precise. Collective private action at the sectoral/industry level can also shape arrangements by proposing standards. This can lead to privately developed standards gaining recognition and, once they achieve critical mass in terms of adoption, ultimately forging a regulatory/legislative pathway to implementation[5].

Singapore's rule on data transfers under Section 26 of the PDPA creates an obligation to 'ensure that organisations provide *a standard of protection* to personal data so transferred *that is comparable* to the protection under' the PDPA[6]. This indicates that the focus is still, as with adequacy decisions, on *standards*, with a need for*comparison* against the PDPA standards.

The section is supplemented by the Personal Data Protection Regulations 2014, which sets out a series of possible routes for organisations looking to transfer data. These include:

- procuring data subject's consent;
- proving that the transfer is necessary to conclude or perform a contract; and
- identifying and applying certain exemptions (e.g. from the consent obligation, publicly available data, data in transit)[7].

But, above all, the execution of legally binding specific agreements between the parties to the cross-border transfers, with terms that regulate their respective obligations in relation to that transfer, is vital.

Scoping private agreements: Four Key Steps

Of course, whenever private agreements are in place, the impact of local law on such agreements will need to be assessed and addressed.

There might very well be, in the process of comparing relevant standards, the issue of making comparisons between divergent national rules. Different local laws might set out different requirements which may include, for example, notifying the transfer to a data protection regulator, taking steps like registering the transfer arrangements for approval, meeting specific obligations and

requiring express/explicit agreement on them between the parties, or using a standardised agreement form.

To navigate competing standards, it will also be important to understand the perspective in play and ask questions such as:

- What is the reason for the transfer?
- Are there safeguards at work?
- Is there a protocol or process to address data breaches or possible risks?
- What might change over time?

The terms and conditions of any agreement might well be a matter of catering to these various facets, and ensuring that there are operational processes which can be applied to complement the contractual safeguards.

This suggests at least the following four key steps should apply in the context of each jurisdiction:

1. Considering whether the cross border transfer arrangements fall within/conform to any categories of permissible cross border data transfer in the originating jurisdiction. This should also include considering what is necessary to ensure that these permissions continue to apply as long as the transfer arrangements are in place.
2. Following through on regulatory steps and coordination (whether in the originating or destination jurisdictions).
3. Supplementing all transfer arrangements with appropriate private agreements and operational processes and safeguards - ensuring that these are appropriate to the nature of transfers in question at all times.
4. Validating the agreements, processes, and safeguards against the laws of the originating and destination jurisdictions alike - both at the outset and then periodically after.

Conclusion

So, is the client's cynicism at the start of this article merited?

Is this complexity all about charging the client more money?

Indeed, it does sound like there are detailed steps to take, agreements to draft, possible permutations to consider. Might that all translate to extra costs?

Like all good lawyers would say: that depends.

Cross-border transfer arrangements have enough variety in them to not quite fit into just one mould.

Some of those moulds are 'cost light' (in that they might be easy to apply without serious lifting on the legal and regulatory side of things - although it is possible that operational safeguards and processes might also have an invoice - or many invoices - of their own[8]).

Yet others might require a more intensive focus to get things in order.

So the devil in the details (or invoice) might be a lot smaller or bigger than originally thought.

But then again, arming yourself with enough knowledge to execute the four key steps mentioned above might help you with getting to know him well.

After all, better the devil you know, than the devil you don't.

Jeffrey Lim Director
jeffrey@joylaw.com
Joyce A. Tan & Partners LLC, Singapore

---

1. The process, and the record of decisions for where the Commission has issued recognition of adequacy (the adequacy decisions) are accessible from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
2. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC
3. *Maximillan Schrems v. Data Protection Commissioner (Ireland)*, 6 October 2015, Case C-362/14, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ03=62, which led to the collapse of the so-called US-EU 'safe harbour' arrangements.
4. For more, see: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en
5. E.g. the Regulatory Pilot Space ('RPS') adopted by the GSMA: https://www.gsma.com/newsroom/press-release/gsma-supports-world-first-in-asia-pacific-for-digital-innovation/
6. Section 26 of the PDPA.
7. Section 9, Personal Data Protection Regulations 2014.
8. The installation of data breach processes, audits, training, investment in IT etc.

RELATED CONTENT

NEWS POST
Spain: AEPD fines HM Hospitales €48,000 for GDPR violations

NEWS POST
EU: Council adopts decision authorising EU-UK negotiations

GUIDANCE NOTE
Denmark - Cookies & Similar Technologies

NEWS POST
Greece: HDPA publishes guidance on cookies

LEGAL RESEARCH
Digital Economy Partnership Agreement (unsigned)