Prepared by AmCham member

HILLBRIDGES

Data protection: A European export

Following the recent "Google case" recognizing the right to be forgotten amid the proposed EU data protection reform possibly introducing changes by year's end, compliant data protection is as relevant as ever. One important compliance aspect not to be overlooked is the transfer of personal data.

What's the deal?

As world markets continue integration, cross-border transfer of personal data practically becomes an inevitable part of data processing. Persons subject to an EU member state's jurisdiction are responsible for ensuring the lawful transfer of personal data pursuant to national law.

In order to duly transfer personal data for processing purposes to a recipient in a non-EU country, the EU data exporter must consider whether the data recipient is in a country which the EU classifies as offering an "adequate level of protection" safeguarding personal data.

When the EU person intends to compliantly transfer personal data to a recipient in a country which is not deemed to offer an "adequate level of protection"– a status held by the US and the majority of non-EU countries – some measures will have to be undertaken by the recipient.

Wisely, strategic EU-based and cross-border businesses are earnestly beginning to implement appropriate personal data protection practices – although not without difficulty.

What's the holdup?

Persons subject to EU personal data protection rules often find difficulty in explaining the data processing and transfer obligations to their non-EU business partners or group-related companies. Indeed, EU persons often struggle to convince the non-EU person that, to the EU data exporter, the threat of sanction for noncompliance is real and potentially substantial. Typically, such pleas for cooperation are met by indifferent disbelief.

Why so?

One obstructing factor is that regulatory approaches to data protection differ internationally. The US and EU, for example, assume entirely different approaches. The US takes an ad hoc "sectoral approach" yet generally favors the right of freedom of speech and access to information, whereas the EU favors a firm right to privacy including a protected right on the processing of personal data. With these regulatory approaches at odds, how can businesses comply?

Choose wisely

In the case of an EU person transferring personal data to the US for processing, three possible methods are currently available absent other specific legal exceptions.

- **US-EU Safe Harbor Program**
  Although under fire, currently, EU data exporters may compliantly transfer personal data to US organizations qualified under the US-EU safe harbor program. In order to qualify, the eligible US organization must comply with all requirements of the US–EU safe harbor framework and generally adopt mechanisms in line with EU data protection rules. Such US organization must annually self-certify compliance with the US Department of Commerce and is then deemed to offer adequate protection, recognized throughout the entire EU.

- **Binding Corporate Rules**
  Multinational companies may adopt binding corporate rules on the protection of personal data to be effective between all of its group members, thereby internally obliging its group structure to comply with EU data processing requirements. This method, occasionally favored by large multinational corporations, can prove rather costly and currently requires prior approval by national data protection authorities. Following approval however, the multinational may transfer personal data world-wide between its group without further hassle. This method is not restricted to US-EU recipients only.

- **Standard Contractual Clauses**
  Also not exclusive to US recipients, the EU-based controller and the non-EU data recipient may contractually adopt EU Commission approved standard contractual clauses concerning the transfer and processing of personal data. When appropriately adopted, the standard contractual clauses facilitate the legitimate cross-border transfer of personal data. Provisions imposed on the non-EU party are rather extensive and deviation from the approved terms of the standard contractual clauses is largely restricted. However, many companies find adopting the standard contractual clauses as the most commercially suitable method for transfer compliance.

Positioning for tomorrow

The nature of data processing changes rapidly due to its inherent connection with technological advancement, and data protection reform aims to keep pace. While some proposed EU reform measures aspire to produce more business-friendly conditions, many of the proposed changes intend to strengthen compliance requirements for all companies doing business with the single EU market.

It has often been said that data protection is made in Europe. The EU has also indicated its intent to raise the world's data protection standards. Although implementing higher regulatory standards may restrict business opportunities, such standards could nevertheless be utilized advantageously.

Companies having a compliant data processing framework will have a competitive advantage because they will be able to assure foreign business partners of compliant data transfers with minimal burden. Additionally, companies with currently compliant data protection operations should be in a better position to readily adopt future obligations, saving time and money.

Companies could take advantage of these standards and develop a high-quality, compliant, and readily adaptable data protection framework to serve as a marketable commodity better positioning them to seize market opportunities, anticipated to considerably increase following a successful finalization of the TTIP agreement.

Anthony P. Hernandez
Associate, Hillbridges