THE NEW EU-JAPAN PERSONAL DATA DEAL: EU AND JAPAN TO EACH RECOGNIZE THE OTHER'S PERSONAL DATA PROTECTION SYSTEM AS EQUIVALENT – WHAT IT MEANS FOR BUSINESSES AND NEXT STEPS

Date: 27 August 2018

EU and Asia Data Protection, Privacy, and Security Alert

By: Yuki Sako, Claude-Étienne Armingaud, Ignasi Guardans

BACKGROUND

On 17 July 2018, the European Union (the "EU") and Japan reached an agreement to recognize each other's data protections systems as "equivalent", and each commits to complete internal procedures by fall 2018 (the "Data Agreement"). Once adopted, this will allow businesses to transfer personal data from the European Economic Area[1] (the "EEA") to Japan and vice versa without being required to provide further additional safeguards for each transfer.

The Data Agreement concludes the two-year-long dialogue regarding mutual recognition of personal data protection regimes between the two parties, and it was issued along with the EU-Japan Economic Partnership Agreement, a long-awaited EU-Japan free trade deal. Prior to the final Data Agreement, in December 2017, the governments issued a joint statement to resolve issues essentially within the existing personal data protection framework to enable free data transfer between the two parties.

THE MECHANISM

EU: GDPR Framework

The EU General Data Protection Regulation 2016/679 (the "GDPR") replaced the Data Protection Directive 95/46/EC on 25 May 2018 and aims at harmonizing data privacy laws across Europe, protecting and empowering all EU residents' data privacy and reshaping the way organizations across the world approach data privacy with an extensive geographical scope.

©2005-2024 K&L Gates LLP. All Rights Reserved.

The GDPR sets new standards for data collection, storage and usage and represents one of the most robust data privacy laws in the world, along with the way such data may be transferred outside of the EU, where lesser standards may apply.

The GDPR extended and clarified the previous territorial scope of European privacy by introducing new applicability criteria. As a result, many companies have found themselves subject to the GDPR's reach.

Indeed, the protection established by the GDPR applies to EU-based companies engaged in processing of natural persons' personal data, regardless of their nationality or place of residence and regardless of whether the processing takes place in the EU or not.[2] In addition, the GDPR also applies to all companies, regardless of their place of establishment, processing personal data of subjects residing within the EU.[3] In this case, the GDPR will apply where the processing relates to the “offering of goods or services” to European residents or where the behaviour of European residents within the EU is “monitored”.

By applying the GDPR to any organization around the world, which would process personal data relating to any data subjects within the EU, Europe is setting itself up as the leading voice on data privacy matters globally. Thus, it is not surprising that more and more companies are becoming highly concerned with the GDPR's potential “spill over” impact on all of their processing and governance considerations.

When a company is subject to the GDPR, all the transfers of personal data outside the EEA are prohibited unless (i) the recipient is located in a zone deemed by the European Commission (the “Commission”) as providing an adequate level of protection for such personal data; (ii) the data controller and processor both provide appropriate safeguards suggested by the Commission; or (iii) where a specific derogation is granted.[4]

Therefore, economic players concerned by the GDPR are in a constant search for ways to facilitate the transfers of personal data outside of the EEA, which are an obvious operational necessity.

An adequacy decision is the most straightforward tool provided under the GDPR to allow the free flow of personal data between EEA members and a third country. Its adoption involves a comprehensive assessment by the Commission of the target country's data protection framework, the relevant redress mechanisms available for individuals and the international commitments or other obligations, in particular in relation to data protection, which must be adhered to by the target country.[5]

The adoption of an adequacy decision implicates: (i) a proposal from the Commission and the approval of the draft decision by the College of Commissioners (the “College”); (ii) an opinion of the European Data Protection Board (an independent body that provides guidance on the application of the GDPR); (iii) the green light from a committee composed of representatives from all EU Member States; (iv) an update of the European Parliament Committee on Civil Liberties, Justice and Home Affairs; and (v) a formal adoption by the College.

Once granted, the adequacy status is not limited in time, but it is reviewed on a regular basis and can be repealed.

The Japan Adequacy Decision

The adequacy decision under the Data Agreement concerns the level of protection granted by the Japanese Personal Information Protection Act (the “PIPA”). To comply with the EU strict standards, Japan committed to

©2005-2024 K&L Gates LLP. All Rights Reserved.

strengthen its rules and agreed to put in place additional safeguards to protect EU citizen's data before the formal adoption of the adequacy decision by the Commission.

In April 2018, Japan's Personal Information Protection Commission (the "PPC"), following the joint statement issued by the two governments in December 2017, released a draft guideline that would apply to the personal data transferred from the EU, which essentially provides additional safeguards (the "Proposed PPC EU Guideline"), and sought for public input. The Proposed PPC EU Guideline includes (i) expanding the base definition of "personal data" and the definition of "sensitive personal information", (ii) ensuring the personal data from the EU being used within the purpose of use identified to the individuals, (iii) enhancing protection for further transfer of EU personal data from Japan, and (iv) narrowing the scope of "de-identifiable personal information".

It should be noted that in the Proposed PPC EU Guideline, the PPC expressly noted that the PPC would have an authority to take appropriate administrative actions for failure of compliance with the safeguards provided therein, citing its general authority provided for cases of immediate infringement of rights and benefits of individuals, even though such safeguards are arguably stricter standards than what the PIPA provides. The PPC is expected to issue the results of such public consultation and the final guideline in the near future.

Japan: PIPA Framework

Under the PIPA, generally, unless one of the limited statutory exceptions or exemptions applies, a business is likely to be required to obtain prior affirmative consent from relevant individuals (as opposed to an opt-out option) to provide personal data to a party outside of Japan. As described in our previous publication,[6] one of the exceptions is that the recipient is located in a country or region designated by the PPC as having personal data protection system equivalent to the standards of the PIPA.

In response to the Data Agreement, the PPC has issued the statement that the Commission has agreed that the EU should satisfy the required standards to be recognized as a region providing equivalent protection as the PIPA and is expected to issue a final order designating the EU as such a region with an equivalent protection system when the EU completes its adequacy determination. For businesses, this means that, going forward, transfer of personal data from Japan to the EU may be arranged with appropriate disclosure of a privacy policy and without obtaining express affirmative consent from relevant individuals.

NEXT STEPS

There is a common will from both sides of the aisle to formally finalize the adequacy finding and create the world's largest area of free flow of data. The Commission aims at adopting the decision in fall 2018, while the PPC will focus on finalising the guideline providing additional safeguards before such formal adoption.

As a final comment, it should be noted that the Data Agreement concerns personal data transfer in between EU and Japan only; any transfer of private data of EU individuals from Japan to other countries, such as the U.S., will require careful consideration of all applicable laws and regulations.

©2005-2024 K&L Gates LLP. All Rights Reserved.

[1] The EEA brings together the EU Member States and the three EFTA (European Free Trade Association) States (Norway, Liechtenstein and Iceland) into a single market that seeks to guarantee the free movement of goods, people, services and capital.
[2] Article 3 (1) of the GDPR.
[3] Article 3 (2) of the GDPR.
[4] Article 49 of the GDPR.
[5] Article 45 (2) of the GDPR.
[6] See “Cross-Border Transfer of Personal Data,” available here.

KEY CONTACTS

YUKI SAKO
COUNSEL

WASHINGTON DC, TOKYO
+1.202.778.9061
YUKI.SAKO@KLGATES.COM

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2024 K&L Gates LLP. All Rights Reserved.