JAPANESE GOVERNMENT'S RECENT FAQS CLARIFY HOW TO RECOGNIZE E-CONTRACT SERVICES UNDER E-SIGNATURE ACT

Date: 1 October 2020

Japan Corporate Alert

By: Aiko Yamada, J. Ryan Dwyer, III

The Ministry of Internal Affairs and Communications, the Ministry of Justice, and the Ministry of Economy, Trade and Industry jointly issued FAQs (the FAQs) regarding the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000, as amended) (the E-Signature Act) on 17 July 2020 and 4 September 2020 to clarify how certain e-contract services should be recognized under the E-Signature Act.

SUMMARY OF FAQS

The E-Signature Act defines "Electronic Signature" (E-Signature) as a signature given on electromagnetically recordable information (1) in order to indicate that the information is created by the person whose signature is affixed, and (2) with the ability to check whether the information is altered.[1] Prior to issuance of the FAQs, it was not clear whether a private e-contract service fulfills requirement (1) above, since the service involves encrypting digital information created by a service user with the service provider's own signing key, and not the service user's signing key, while the encryption requires the service user's instruction.

The first FAQ dated 17 July 2020 clarified that:

- If encryption technology and functions ensure that information is encrypted automatically, only with the intention of a service user and with no possibility of the intention of a service provider intervening in the encryption process, the service user rather than the service provider might be regarded as "a person giving the signature," which is requirement (1); and
- If a collective review on the overall process including certain confirmable affiliated items (e.g., date and time of sending the information to the service provider) under the e-contract service makes clear that the information is encrypted with the intention of the service user, the e-contract service, viewed as a whole, may fulfill requirement (1).

Accordingly, from this FAQ we can understand that an E-Signature may be regarded as effective if the above two bullets are satisfied by a particular service provider's service.

As an issue separate from the above, the E-Signature Act establishes a presumption of authenticity of the electromagnetically-recorded information, which qualifies if the information has an E-Signature (as defined above) that (a) is given with the personal intention of a person creating the information itself, and (b) is accessible only by the person (Requirement of Uniqueness) (c) through appropriately managing codes and items that are necessary for having the E-Signature given on.[2] Before the second FAQ (see below) was issued, it had not been clear

whether and how an e-contract service may fulfill these requirements, in particular (b) the Requirement of Uniqueness.

The second FAQ dated 4 September 2020 commented that the Requirement of Uniqueness is mandatory to rationalize the presumption of authenticity and also clarified that, while reserving the courts' right to determine at their discretion whether an e-contract service fulfils the Requirement of Uniqueness on a case-by-case basis, the e-contract service might be generally able to fulfill the Requirement of Uniqueness by showing a list of publications for reference issued by certain institutions or organizations (e.g., National Institute of Standards and Technology (NIST), Cryptography Research and Evaluation Committees (CRYPTREC)), as well as some other views and factors to consider, such as:

- Process to be established between a service user and a service provider: An adequate identification system is required to be established and maintained. A two-step authentication process, among others, might be an example of an adequate identification system.
- Process to be established within a service provider: An adequate security system is required to be established and maintained. Capabilities and functions to ensure high-strength encryption and accurate linkage to each user, among others, might be an example of the adequate security system.

The second FAQ also clarified that:

- To fulfill the requirement (a) above, it is critical that the user of an e-contract service is confirmed to be identical to the person creating the information.
- “Appropriately managing codes and items that are necessary for having the E-Signature given” (the requirement (c) above) might include, without limitation, appropriate management of a service provider's signing key, a service user's password, a server, and a smartphone or token to be used for a two-step authentication.

TAKEAWAYS

Under the Civil Code of Japan, any style of contract may be legally binding on the parties as long as their assent to be bound can be shown (unless otherwise required by a specific law), and therefore any contract created through an e-contract service (e-contract) could be legally valid. However, parties may not completely exclude the risk that the validity of a contract is disputed at the court, and therefore it may be critical to establish the presumption of authenticity of the e-contract by fulfilling all the requirements set out in the second FAQ as discussed above.

There are various e-contract services currently available. When parties wish to introduce use of a certain e-contract service from among other similar e-contract services for material contracts, they would be well advised to carefully compare each offering with an eye to picking one that may fulfill these requirements.

In the case of cross-border transactions between international parties, the situation would likely be more complex. Parties should keep in mind e-contract or e-signature regulations in each relevant jurisdiction to mitigate the risk that validity of the e-contract is challenged or denied. Cross-border data transfer regulations would also have to be reviewed and complied with on a country-to-county basis.

This alert is issued for an informational purposes only. Please do not take it as legal advice. For more information regarding this topic or any other related issues, the K&L Gates Tokyo office is available to assist. We are happy to discuss any of the above points further. To learn more, please visit our office page.

FOOTNOTES

[1] Article 2(1) of E-Signature Act.

[2] Article 3 of E-Signature Act.

KEY CONTACTS

AIKO YAMADA
COUNSEL

TOKYO
+81.3.6205.3630
AIKO.YAMADA@KLGATES.COM

J. RYAN DWYER, III
PARTNER

TOKYO
+81.3.6205.3601
RYAN.DWYER@KLGATES.COM

