Comparative Overview of GDPR and Japanese Privacy Act

Even if a mutual recognition of adequate standards for data protection is expected and likely to happen within the biennium 2018-2019[1], some differences between the two legal regimes still remain[2]. The comparison between the new reformed acts (GDPR and Japan's Personal Information Act) that is carried out below elicits a number of differences which give an example of the potentially significant operational efforts and compliance demands on businesses and organizations wanting to make benefit of the opportunity of both European and Japanese data markets[3]. Nevertheless, the proximity of both reforms and the fact that both were approved over the last years supports the argument that "(. . .) the significance of the differences is less"[4].

Territorial scope
With reference to the territorial scope, the GDPR details the extraterritoriality principle[5] (present in both jurisdictions) with an additional point. Such a principle implies that the legal standards set up within the territory by the GDPR do also apply outside such territories as long as foreign businesses and organizations offer goods and services to within the country or territory where the data protection laws apply. Thus, both territories of the European Union and Japan extend the applicability of their privacy laws to those established abroad but with the above-mentioned business interests within such regions. However, GDPR further extends such applicability also to those firms, which are not established within the EU but monitor European data subject's behaviors.
Personal information
Whilst the GDPR considers personal information as those relating to an identified or an identifiable person[6], the Japanese Act differs in such definition as follows. For such a concept in fact, the Japanese Personal Information Act provides a slightly divergent notion, i.e. those information relating to a living individual, which can identify such specific individual by the description contained in the information. Additionally, the Japanese Act adds up a definition of personal data, i.e. those personal information that are processed within a database (with dedicated rules[7] and procedures for such cluster of personal information).

[1] Kensaku Takase , *GDPR matchup: Japan's Act on the Protection of Personal Information*, IAPP, 29.8.2017
[2] Mark Scott and Laurens Cerulus, *Europe's new data protection rules export privacy standards world- wide*, Politico.eu, 6.2.2018
[3] Ibid: see footnote 1
[4] Ibid: see footnote 1
[5] GDPR, Article 3
[6] GDPR, Article 4
[7] Ibid.: see footnote 1

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016).
The information reflects only the views of the project owner.

Sensitive personal information
The list of sensitive personal information under the GDPR is comprised of those revealing ethnic or racial origins, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic or biometric data for identification purposes. The Japanese Act includes in its list information concerning religion, social status or medical history, criminal records and the circumstance where a data subject has suffered damages from a crime[8]. Such narrower interpretation of the category of sensitive personal information by the Japanese laws has allegedly caused some delays during the negotiations[9], since the European approach protects in this category trade union memberships and sexual orientations, whilst the Japanese Act does not[10].
Information rights
With respect to data subjects' rights, the Japanese Act distinguishes between the duty of data controllers to provide for disclosure, rectification or cease of processing, added by the obligation of explanation of reasons (within the obligations chapter). The GDPR enlists a number of more systematic rights, such as the rights of information, access, rectification, erasure, object and explanation. On top of such basic rights, the GDPR improves user controls over his or her data by adding a new right at Article 20 (currently absent in the Japanese provisions): the right to data portability[11].
Data controllers and processors
Unlike the European Union, which has a longstanding tradition in the use of the term "data controller" within its privacy laws, Japan does not seem to have a perfectly overlapping profile. Such concept is in fact replaced in the Personal Information Act by the notion of "business operator"[12], which is the responsible entity for the handling of the information. No further distinction with personal data processors is made in the law.
Penalties and fines
The GDPR raises the bar for potential violation of its provisions up to 20M Euros or 4% of the global annual turnover. However, no criminal liability arises from the regulation. Conversely, the Japanese Act has a lower breach sanctions cap (for instance, for database stealing, the fine is up to 500,000 Yen, roughly 4,200 Euros), while explicitly foreseeing up to one-year imprisonment.

[8] Ibid.: see footnote 1

[9] Julia Fioretti, *EU sees data transfer deal with Japan early next year*, Reuters, 15.12.2017

[10] IAPP, *EU-Japan data protection talks positive, some differences remain*, 18.12.2017

[11] "The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services". The Information Commissioner's Office (ICO), Right to data portability, www.ico.org.uk , last accessed 19.3.2018

[12] Ibid. see footnote 1

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016).
The information reflects only the views of the project owner.