ISSN 2644-237X
DECEMBER 02, 2019 CIOREVIEW.COM

CIO Review

The Navigator for Enterprise Solutions

EUROPE SPECIAL

GDPR EDITION

AI: The New Guardian of Data Security

László György Dellei, CEO

KERUBIEL

$ 15U S

THE LONG ARM OF *THE PRIVACY REGULATION*

By Ozan Karaduman, Partner, Gün + Partners

GDPR has been one of the most important regulations for the companies in Europe and also some of the companies in other countries. However, Europe is not the only jurisdiction with a privacy regulation. Various other countries like Turkey, Japan, South Korea, and Australia have privacy laws. A company located in Europe has to take into account the provisions of both the GDPR and the privacy regulations of other countries where it does business. For example, when there is a data breach, the European company may need to notify both the supervisory authority in Europe and the supervisory authority in the other countries if it processes personal data of the residents of those other countries.

The extraterritorial reach of the privacy legislations in various countries is not limited to data breach issues. Other provisions in privacy laws in various jurisdictions may be applicable to a European company even if such company does not have an actual presence (e.g. a subsidiary or a branch) in those jurisdictions. In those cases, the interaction between the GDPR and the applicable privacy law in the relevant jurisdiction plays an important role for the company to find its path to compliance.

Analysing all of the provisions where the provisions of the GDPR may interact with those in the other jurisdictions would be beyond the scope of this article. Therefore, we will take the information obligation in the GDPR as an example and briefly analyse how a privacy notice must be prepared by a European company in a jurisdiction which has its own privacy laws that may be applied to data controllers located abroad.

One of the most important steps that a European company must take in terms of privacy compliance is to determine the countries of the data subjects whose personal data is processed by that company. The European company should then determine if those countries have privacy laws that have an extraterritorial reach and the scope of the extraterritoriality. In certain jurisdictions, the law maker may want to protect the privacy of the data subjects in its jurisdiction, regardless of where the data controller is located. In such a jurisdiction, the European data controller would need to comply with both the provisions of the GDPR and the provisions of the relevant privacy law in that jurisdiction.

If a company located in France processes personal data of the residents in a jurisdiction that requires foreign data controllers to inform that data subjects in its jurisdiction about its data processing activities; within the context of the privacy notice to be sent to the data subjects resident in that jurisdiction; that company will need to comply with both Articles 12, 13 and 14 of the GDPR and the privacy notice obligations in that jurisdiction.

If the obligations related to privacy notice are very different between the GDPR and the relevant jurisdiction, the most direct option might be to prepare two separate privacy notices; one for the GDPR and the other for the relevant jurisdiction. However, this would create an extra burden on the data controller for sending the notices and keeping the logs.

If the obligations related to data privacy notice are similar between the GDPR and the relevant jurisdiction, the data controller may prepare a single privacy notice. However, this is not an easy task; although the categories to be included in the privacy notice under the GDPR and the relevant jurisdiction may be similar, the content of those categories may be different. For example, both the GDPR and the relevant jurisdiction may require the data controller to inform the data subject of the legal basis of the data processing activity, yet the legal basis required by the GDPR and the relevant jurisdiction might be different. For the same processing activity, the GDPR may allow processing on the basis of scientific research whereas the relevant jurisdiction may allow such processing activity only on the basis of explicit consent. In such cases, the data controller would need to determine which legal basis it must rely on in the relevant jurisdiction and insert that legal basis in the privacy notice. The solution might be even more complicated for certain issues such as data transfers abroad. In a GDPR privacy notice, the data controller would need to explain the data transfers out of EEA, whereas the relevant jurisdiction would not be a part of the EEA and would require the privacy notice to mention the data transfers outside the relevant jurisdictions. The mechanisms for data transfers abroad might be different as well. In that type of situations, the data controller would need to include explanations for both cases.

“One of the most important steps that a European company must take in terms of privacy compliance is to determine the countries of the data subjects whose personal data is processed by that company.”

The above is a small example to give a glimpse of the complexity of the situation where both the GDPR and another privacy law are applicable at the same time. More and more jurisdictions test the limits of their territorial reach. The data controllers in Europe should not think that they would only need to comply with the GDPR nor that compliance with the GDPR would automatically mean compliance with the privacy laws in other jurisdictions. They need to make proper legal and operational analyses to determine if they must comply with other privacy laws in addition to the GDPR and how to comply with them. CR