THE
NATIONAL LAW REVIEW

Transfer, But How? Cross-Border Flow of Personal Data Under EU Data Protection Directive

SQUIRE PATTON BOGGS
Article By
Ewelina Witek
Squire Patton Boggs (US) LLP
O-I-CEE!

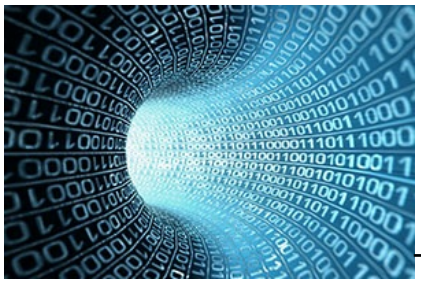
- Communications, Media & Internet
- Global
- European Union

Wednesday, July 26, 2017

In a globalized world, the ability to transfer data between organizations located in different parts of the world is of the utmost importance.

The EU Data Protection Directive (GDPR), which will apply from 25 May 2018, governs the international transfer of personal data.

Data Transfer Within the EU



The free exchange of personal data between member states is a fundamental part of the EU's basic principles. It arises from the four fundamental freedoms, i.e., the free movement of people, goods, services and capital. This principle is also reflected in the GDPR, which excludes the restriction or prohibition of the free movement of personal data within the EU or, even more broadly, within the EEA.

Data Transfer to Third Countries

Different rules apply when transferring data to a third country. GDPR does not define the term “third country”, but it should be assumed that this is a non-EEA country, such as the US and India.

Transfer of data to a third country occurs when it is made beyond EEA boundaries (e.g. data transfer via e-mail), regardless of whether the data will then be actively used (e.g. changed, deleted) or only stored (e.g. when the transfer took place for the purposes of storing them on servers located in India).

Basis for Cross-border Data Transfers

With regard to data transfers to a third country, the GDPR introduces specific rules, i.e.,:

- Data transfers to a third country can only be carried out on the basis of a decision by the European Commission establishing that a given third country, territory or sector ensures an adequate level of protection (currently such decisions are issued for Argentina, Israel, Canada, New Zealand, Switzerland and will remain in force under the GDPR until repealed or amended; for data transfers to the US, the Privacy Shield program applies on a self-certification basis – entities that participate in the program are considered to ensure an adequate level of data protection).

- In the absence of a relevant decision by the European Commission, the transfer of data to a third country without the need for the data protection authority’s consent may take place only if adequate safeguards are provided, such as the use of Binding Corporate Rules (BCR) approved by the competent authority for the protection of personal data (a solution particularly favorable for international corporations) or standard contractual clauses adopted by the European Commission (controller-controller or controller-processor clauses) or the use of an approved code of conduct or certification mechanism.

- In the absence of a relevant decision by the European Commission, the transfer of data to a third country may take place with the permission of the data protection authority, e.g., under an ad hoc contractual clause between the controller or the processor and the controller or processor in the third country.

- When it is not possible to use the above mentioned options, transfer of data to a third country can only occur once the conditions set out in Article 49 of GDPR, which provides for derogations (exceptions) in special situations, are met. Those derogations include, e.g., the explicit and voluntary consent of the data subject for the proposed transfer, after having been informed of the possible risks of such transfers for the data subject, necessity of data transfer for the performance of a contract between the data subject and the controller, or necessity of data transfer for the exercise or defence of legal claims.

Priorities

When personal data is transferred to third countries, a priority should be given to the solutions described in the first three paragraphs above. As a result, the data is protected on the basis of the safeguards arising from the abovementioned instruments, even where it is transferred to a third country that does not provide an adequate level of protection. Only in exceptional cases – e.g., if data protection is impossible to be ensured or it is disproportionately difficult, or where the risk of infringement of the rights of the data subject is negligible – may the derogations provided for in Art. 49 of GDPR, described in the last paragraph above, be introduced.

Avoiding the Punishment

Finally, it is worth mentioning that the transfer of data to third countries without a proper legal basis is subject to a high administrative fine – up to €20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

It is, therefore, of the utmost importance to check **as soon as possible** the basis for data transfer and possible implementation of appropriate regulations.