CROSS-BORDER DATA TRANSFER

Are there any restrictions on transferring personal data and how can these be overcome?

Cross-border data transfers affect all organizations that engage online IT services, cloud-based services, remote access services and global HR databases. Understanding the applications of lawful data transfer mechanisms is essential to validate recipients located outside the European Union (EU).

Data transfers typically include the following examples:

- personal data communicated over the telephone, by email, fax, letter, through a web tool or in person to a country outside the EU;
- IT systems or data feeds which lead to personal data being stored on databases hosted outside the EU;
- people/entities outside the EU being able to access or "see" personal data held in the EU; and
- the use of personal data by third parties through external solutions, e.g., outsourcing, offshoring and cloud computing.

First, it is important to note that the transfer of personal data to a third country or an international organization is possible. The transfer is legally allowed where the EU Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. A transfer based on a decision of adequacy shall not require any specific authorization.

In the absence of a decision of adequacy, the personal data transfer to a third country may take place if appropriate safeguards are in place, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The GDPR enforced adequacy mechanisms that were already adopted in the previous Directive, such as:

- **Binding Corporate Rules** (BCR): personal data protection policies offer clear sets of rules for businesses engaged in a join economic activity. They are adhered to by a controller or processor established in the EU territory for transfers of personal data to a controller or processor in one or more third countries.

The BCR must contain: privacy principles (transparency, data quality, security, etc.); tools of effectiveness (audit, training, complaint handling system, etc.); and an element proving that BCR are binding.

The BCR must be submitted to the data protection authority, and will be amended in collaboration with other data protection authorities. The entire approval process has no established timeframe.

- **Standard Contractual Clauses** (SCC): clauses that offer sufficient safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.

The EU Commission has so far issued two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU, and one set for the transfer to processors established outside the EU.

The set "controller (EU) and processor (non-EU)" has been also used as the SCC for processors and sub-processors. The GDPR mentions the addition of new SCC for processors and sub-processors. Such clauses

are not yet approved but there is a draft available for consultation.[1]

The purpose of the SCC "is to facilitate the task of processors in the implementation of transfer contracts." Therefore, each new contract must come with SCC. The SCC are not subjected to any authorities' approval, the main reason why their content cannot be modified. If changes are made, the parties must submit the document for data protection authority approval.

While SCC generally work well for smaller companies and bilateral data sharing, they might not fit precisely where there is a complex web of processing, and the growth of affiliates abroad may lead to the need to put in place hundreds of SCC.

Adopting BCR and SCC allows organizations to harmonize practices relating to the protection of personal data within a group, avoid the need for a contract for each single transfer, communicate externally on the company's data protection policy, have an internal guide for employees with regard to personal data management, and make data protection integral to the way the company carries out its business.

HR Best Practices: For intragroup transfers (such as access from a subsidiary outside the EU), make sure to have at least one safeguard mechanism in place: BCR "Controller to Controller" or SCC signed with the concerned subsidiary. For cross-border data transfer with processors or sub-processors, make sure such collaborators have their own safeguard mechanisms in place.

The use of applications in the cloud frequently results in the international transfer of employee data. Personal data should only be transferred outside the EU when an adequate level of protection is ensured and access by subsequent entities remains limited to the minimum necessary for the intended purpose.

Last updated June 2018.

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf