In an economy where borders have virtually dissolved, companies increasingly need to exchange information at a global scale. Companies make personal information available across borders to manage their IT systems, centralize their human resources databases, exchange customer files, store information in shared data centers, or migrate their information systems to the cloud. However, such information transfers are subject to restrictions, which, if not observed, may expose companies to important liability risks. This article discusses these restrictions on data transfers under current European (EU) laws and explains why companies are increasingly regarding Binding Corporate Rules (BCRs) as a successful solution to managing their data privacy compliance while securing their international data flows. This article is the first of a series of four.

Exchange of information within a corporate group is subject to significant restrictions under EU laws.

Most transfer options are onerous or come with legal uncertainty.

Companies increasingly consider adopting Binding Corporate Rules (BCRs) to manage their data privacy compliance and secure their information exchange.

BCRs offer flexibility and create a culture of trust within a company and vis-a-vis consumers.

BCRs allow meaningful streamlining of privacy policies and processes throughout a global organization.

Current options for companies in the EU to export personal information

EU data privacy laws and regulations require that individuals benefit from an adequate level of data protection when their personal information is sent outside the EU. The EU Commission has, over time, issued a white list of countries that are considered to provide adequate data protection. Companies located in these countries may receive personal information from data exporters located in the EU. Examples of white listed countries are Israel, Argentina, Switzerland, and Canada. Other adequacy mechanisms allowing the export of personal information

by Jan Dhont, Alyssa Cervantes, and Delphine Charlot

From data transfer solution to privacy compliance strategy

Exchange of information within a corporate group is subject to significant restrictions under EU laws.

Most transfer options are onerous or come with legal uncertainty.

Companies increasingly consider adopting Binding Corporate Rules (BCRs) to manage their data privacy compliance and secure their information exchange.

BCRs offer flexibility and create a culture of trust within a company and vis-a-vis consumers.

BCRs allow meaningful streamlining of privacy policies and processes throughout a global organization.
include EU Commission model contracts, Safe Harbor certification, individuals’ consent, and specific exemptions.

The EU model contracts are contracts that stipulate specific obligations for the data exporter and data importer to exchange personal information. These terms can be included in (or attached to) a service agreement, but cannot be amended if companies intend to export personal information outside the EU.

Alternatively, US companies may rely on the Safe Harbor scheme, which is a self-certification solution provided by the Department of Commerce in consultation with the EU Commission. The Safe Harbor framework is an example of a framework that has been recognized by the EU Commission as providing an adequate level of protection for data transfers similar to the above mentioned white listed countries.

Companies may also rely on the individuals’ consent or invoke legal exemptions to export personal information, such as the necessity to transfer personal information in light of contractual obligations in the interest of said individual.

**Compliance issues relating to intra-group transfers of personal information**

Each data transfer solution presents some advantages but also bears some limitations. Although model contracts appear at first sight to provide for an easy transfer solution, companies located in jurisdictions that have no or few developed data privacy laws may not be willing to accept their terms. Furthermore, the execution process is often onerous in practice, especially if many contract parties are involved at the data exporter and data importer side. In addition, companies located in the EU that use these model contracts are required to apply for a data transfer permit in some jurisdictions (e.g., Spain, Denmark, Portugal), which can be time-consuming and costly.

Next, the Safe Harbor framework is only available to US organizations that import personal information from the EU. What is more, Safe Harbor has been under permanent criticism since the Snowden revelations and is subject to ongoing US-EU reform discussions. The Safe Harbor framework is only available to US organizations that import personal information from the EU. What is more, Safe Harbor has been under permanent criticism since the Snowden revelations and is subject to ongoing US-EU reform discussions. The Consortium of EU Data Privacy Authorities (WP29) has recently threatened that “[i]f the revision process currently undertaken by the EU Commission does not lead to a positive outcome, then the Safe Harbor agreement should be suspended and recalled that, in any case, data protection authorities may suspend data flows according to their national competence and EU law.”

In turn, US service providers that rely on Safe Harbor are increasingly finding themselves stuck in deal negotiations with customers who refuse to contract with them unless they implement a different solution.
Consequently, obtaining direct consent from individuals may seem like the perfect option. However, obtaining an individual's consent often comes with legal uncertainty. This is mainly due to the fact that an individual may revoke his/her consent at any time. Furthermore, in most EU countries, consent should be free and informed. But employees, for instance, will rarely be regarded as being in a position to provide free consent towards their employer.

**Why should companies consider BCRs?**

Binding Corporate Rules (BCRs) are a set of rules that set forth a data privacy regime to exchange personal information within a group of companies. They are a co-regulatory initiative developed by multinational companies (such as GE and Philips), which gained gradual support by national data privacy authorities (DPAs). They take the form of a code of conduct backed by policies, procedures, and control mechanisms, which are negotiated and approved by the national DPAs.

DPAs originally were not collectively supportive of BCRs, but the political context has changed dramatically over the last years. Currently, 66 companies have obtained BCR status, and nearly as many applications are currently pending. This is primarily due to the facts that: (1) DPAs have increasingly gained experience dealing with the approval process and consider BCRs as a trustful token of privacy compliance; (2) BCRs create trust among employees and consumers; (3) BCRs allow meaningful streamlining of privacy policies and processes throughout a global organization; and (4) BCRs constitute an ideal preparation for compliance with the nearby European Data Privacy Regulation, which will constitute an overhaul of the current European data privacy framework.

**Are you ready for the new Data Privacy Regulation?**

Companies should consider rendering their information practices future-proof in view of the adoption of the Data Privacy Regulation expected by the end of this year. To become legally effective, the draft regulation still needs to be approved by the European Council. In a meeting of the Justice and Home Affairs Council in Brussels on March 13, 2015, EU Member States declared that they are ready to wrap up their first reading of the new regulation by June 2015. The use of BCRs by companies appears all the more likely as the new regulation expressly acknowledges BCRs as a valid transfer solution. In the following articles, we will address the content of the BCRs, discuss the advantages and disadvantages of the BCRs, and explain the application and approval process.

---


Jan Dhont (J.Dhont@koanlorenz.com) is Partner and Head of the Privacy and Data Protection Practice at Koan Lorenz Law Firm, Brussels. Alyssa Cervantes (A.Cervantes@koanlorenz.com) and Delphine Charlot (D.Charlot@koanlorenz.com) are Associates in the Privacy and Data Protection Practice at Koan Lorenz Law Firm, Brussels.