Dancing the legal limbo around US/EU data transfers

Difficulties often manifest themselves in transferring data from the ‘safe’ EU to the ‘unsafe’ US. Difficulties also exist with US law enforcement authority requests for access to such data, which is often not permitted under EU law. Jana Fuchs, an Associate with Bryan Cave LLP, examines the problem and potential solutions.

When a Chief Privacy Officer (CPO) is finally able to check the box to ‘implement sufficient EU data protection adequacy measures for data transfers,’ nerves are often frayed and a level of frustration remains. For global companies, the path to centralise data management (e.g., allowing HR or customer data to be transferred and controlled in ‘unsafe’ countries such as the US) exists, but traversing it can be rocky.

**EU originating personal data controlled abroad**

The first thing that often comes to mind is the EU-US Safe Harbor framework. One of the first lessons that they learn is that the ‘Safe Harbor’ is not so safe at all. When they look to other commonly discussed routes to compliance, similar drawbacks start to emerge. Model Contracts have significant grey-zones, and the EU approved Binding Corporate Rules (BCR) can conflict with national compliance requirements applicable to US data importers.

The EU cross-border data transfer system was established decades ago (in particular, before the US Patriot Act) and grey-zones are unfortunately the rule and not the exception, for example, the processing and onward transfer of personal data received from the EU in connection with national mandatory compliance measures once such data is being controlled in the US. This article examines the problems that can occur once data has been imported in to the US and is controlled by a US entity.

Similar issues arise when, for example, US law enforcement or a dispute party requests the transfer of data directly from the EU, e.g. in an e-discovery scenario from a subsidiary in the EU. The direct access enforcement is limited, as opposed to those situations where the concerned data is already controlled in the US.

**Uncertain legal framework**

US companies with data processing that is exempt from the Safe Harbor framework (e.g. companies in the financial sector) have to deal with uncertain regulations and a legal framework based not only legal interpretation, but also emotional reaction. Many of the concerns and criticism that arise in the context of data transfer are based on a lack of trust in the existing legal framework for data transfers that arises as much from the media’s disclosure of spying activities from the National Security Agency, as from any explicit legal document or concern.

To provide background, personal data that originates from the EU, but is controlled in the US, remains subject to the EU data protection principles through the chosen EU adequacy tool (e.g. Safe Harbor, Model Contracts, or Binding Corporate Rules). At the same time, the US data importer, as well as any data processing by the importer, are also subject to applicable US laws and are more susceptible to US law enforcement agencies applying those laws. The EU legislation, whether on the EU or the Member State level, often does not provide clear guidance as to how a company can, or should, comply with US laws that may require that information be disclosed; conversely US laws focus on national US interests, often with little acceptance or recognition of EU privacy restrictions.

**US disclosure requirements**

Companies controlling EU data can be confronted with access requests from US law enforcement, evidence discovery obligations from US courts, or administrative subpoenas from US agencies also affecting controlled EU personal data. Many US companies are required to investigate issues that may implicate data originating in the EU. Anti-corruption or anti-money laundering investigations often require examining EU personal data controlled in the US to be complete. None of the US legal obligations provide a carve-out for data that originates in the EU, or that may be subject to EU privacy protections.

The conflict with EU privacy protection is real and direct. For example, onward transfer of EU originating personal data to another data controller is generally prohibited, unless certain conditions are met. Allowing e.g. a US security authority access to EU data is by EU standards considered an onward transfer of data to another data controller.

**EU Model Contracts**

Model Contracts’ generally set out a ‘Notice, Adequacy or Choice’ principle. The Safe Harbor restrictions could be summarised as a ‘Notice, Choice and Adequacy’ principle, generally requiring opt-out consent for onward transfers.

For Model Contracts, this approach means that the data importer shall not disclose or transfer personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies (gives ‘Notice’ to) the data exporter, and:

- the third party data controller processes the personal data in...
accordance with a Commission decision finding that a third country provides adequate protection ('Adequacy');
● the third party data controller is a signatory to these clauses or another data transfer agreement approved by a competent EU authority ('Adequacy');
● data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards ('Choice'); or
● with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer ('Choice').

In law enforcement requests, this means that a data controller may be prohibited from providing EU data to a US law enforcement agency. Where Safe Harbor is not applicable, e.g. to some extent in the US financial sector or outside the US, Model Clauses are often the only direct source of guidance for cross border data transfers.

To summarise, the common basis for Non-EU data controllers controlling EU data is that onward transfers, i.e. also access by a law enforcement institutions, is prohibited, unless:
● the receiving entity ensures an adequate level of data security by EU standards; or
● the concerned data subjects have been given the option to object.

Both regulatory options are hardly reliable solutions.

**US provision of ‘Safe Harbor’ for EU data**

It is unlikely that the receiving US law enforcement authority or a US court accepts compliance with, for example the Safe Harbor principles or enters into an EU Model Contract. Also, a reliable consent from the concerned data subjects will be difficult, if not impossible, to obtain for these kinds of purposes. Valid consent by EU standards requires free choice as well as withdrawal rights, which is usually contrary to the authority's purpose for accessing the data. Furthermore, the dependent position of, for example employees, limiting free choice, would always have to be considered even if consent was given.

Another approach to justify US compliance measures is based on the access exemption stipulated in the Set II ‘Controller to Controller’ Model Clauses or similar exceptions under Safe Harbor. Here, the rules confirm the 'Adequacy Principle,' by stating that the data importer shall have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. However, an exemption for access required by law is constituted, by saying that this provision shall not apply to persons authorised or required by law or regulation to have access to the personal data.

Given the broad scope of this exemption, it is often quoted as a basis for allowing third party access to personal data originating from the EU; when such is deemed necessary for legal reasons by the data importer. However, from the EU perspective, the scope of this exemption is subject to a highly controversial discussion and the legal effects are often uncertain.

A broad interpretation of this exemption is likely, defeating the restrictions under the EU data protection measures, as well as the purpose of extending the EU security standards to EU data controlled in the US. Thus, a broad interpretation would likely not be accepted by EU data protection supervisory authorities, who have direct enforcement competence in regard to the EU data exporter.

Generally, the EU data protection enforcement authorities are very reluctant to accept this clause as a reliable justification for granting access to such data. It depends very much on the individual case and the concerned privacy interests need to be thoroughly evaluated and assessed in proportion to the purpose of the intended access.

US companies often find no legal option for complying with their national law enforcement requirements and the EU data protection regime. An example is compliance requirements leading to data screenings in connection with USA Patriot Act enforcement or internal investigations examining other extra-territorial US law, e.g. the Foreign Corruption Practice Act (FCPA).

**Compliance measures in the financial sector are essential**

Companies operating in the financial sector must ensure a very close grid of compliance supervision. And this requirement does not cease at the US border, but extends far beyond that.

Should any personal data originating from the EU, which was gathered e.g. through an internal investigation be transferred to a US authority/court, it is wise to review and document the privacy aspects of such transfer. Companies should be prepared to learn that due to conflicting laws, they might not be able to obey all legal obligations.

While some internationally shared compliance purposes, such as anti-corruption or anti-money laundering, may be more accepted by EU data protection authorities to serve to some extent as justification for onward transfers, this is dependent on the individual case. Other more US focused laws on anti-terrorism or export control
Valid consent by EU standards requires free choice as well as withdrawal rights, which is usually contrary to the authority’s purpose for accessing the data of personal data. Data that has not been collected can neither be transferred nor accessed, data that is anonymised generally falls outside EU privacy laws.

As a second step, it is always worth considering approved BCR, especially for global companies exempt from Safe Harbor. Conflict situations with US regulation can, to some extent, be included in BCR and those could serve as basis for a more reliable framework vis-à-vis EU Data Protection Authorities.

While BCR primarily regulate data flows within a group of companies, the restriction of data transfers/ondward transfers outside the group is a mandatory element of BCR. It is required to include measures to restrict transfers and onward transfers outside of the group and a commitment that all transfers of personal data to external controllers located outside of the EU must respect the European legal framework on cross-border data flows.

The legal framework is set out in Article 25 and Article 26 of the EU Data Protection Directive’. For non-EU entities controlling EU data, this general legal framework could offer a bit more flexibility, because it integrates the general set of data transfer exemptions rather than the further limited and to some extent unclear conditions - for example under the Model Clauses or Safe Harbor. Within BCR, the general framework rules can be designed to better meet the individual data transfer needs of the concerned company.

In Article 25, the EU Directive generally bars the transfer of data from the EU to a country lacking adequate protection of personal data, like the US. Article 26, however, defines exemptions from this general prohibition and sets out exceptional possibilities for the transfer of data from the EU to another country not being regarded as having an adequate level of data protection. These derogations are generally not directly part of Safe Harbor or the EU Model Contracts, as they follow a contractual ‘Notice, Choice, Adequacy’ principle.

All new?
The legal framework for data transfers and its restrictions are also subject to the proposed EU privacy reform. There is a clear tendency to further regulate and restrict onward transfer of personal data and to clarify, for example, that any access to personal data originating from the EU - especially by foreign law enforcement, courts or private parties by way of exemption - may only be justified by EU laws and standards and not, for example, by US national security requirements.

BCRs to master the limbo challenge
The key tool to avoid conflicts arising from contradicting legal concepts is a precise and consequent data limitation concept and, wherever possible, the anonymisation/pseudonymisation

(ITAR) will likely not be accepted.

Employee screenings
Another typical example in the financial sector is the screening of employee data once it is being controlled, for example, in the US. The employee data transferred to the US may only be used and processed for very specific purposes as set out beforehand, e.g. in the EU Model Data Transfer Agreement. US specific national security purposes, for example, are not generally part of that.

It is therefore often difficult, if not impossible, to find a legal basis for such screenings insofar as those are based on national law only, and exceed what is acceptable under the general EU data protection principles. Where an intended screening measure affects EU employee data, the concerned privacy aspects should be thoroughly analysed beforehand in order to avoid risk exposure, in particular to the data exporter.

Jana Fuchs
Associate
Bryan Cave LLP
jana.fuchs@bryancave.com

2. See Set II Controller to Controller Model Clauses, sec. II lit b).