How EU data protection laws impact cross-border FCPA investigations

The Global Anti-Corruption Perspective

24 SEP 2014
By: Carol A. F. Umhoefer

EU data protection laws apply to "personal data" in the broadest sense. For instance, a business email sent by an employee from the office constitutes "personal data" as long as the email directly or indirectly identifies an individual − which is nearly always the case, if only because the email address and the signature include at least two persons' names, sender and recipient.

EU data protection laws encompass a number of principles that are easy to grasp in the abstract.

- Persons whose data are processed must be given ***notice*** of the processing, and must be given ***access*** to their data upon demand
- Persons whose data are processed must give explicit ***permission*** to processing of their data
- The data processed must be ***accurate***
- The data processed must be ***limited*** to only that which is necessary for the purposes pursued
- The purpose of that processing must be fair and ***lawful***
- Data may only be shared with persons located in ***countries that afford adequate protection to data*** in the eyes of the European Commission.

Applying those principles in practice, particularly in the context of a cross-border FCPA investigation, is not necessarily straightforward. Just a few examples:

- Providing *notice* to wrongdoers will tip them off that an investigation has started.
- Wrongdoers may not wish to give *permission* to processing of their data.
- Data uncovered in an investigation may not be *accurate* but nonetheless may serve as the basis for allegations against a suspected wrongdoer.
- When looking for evidence, exculpatory or otherwise, it may be technologically impossible to examine *limited* data.
- Non-EU legal requirements or requests from non-EU authorities do not overrule EU data protection laws and consequently may not be *lawful*.
- *The US is not considered to provide adequate protection to data*, so any transfer of investigation data from the EU to the US may conflict with EU data protection laws.

Clearly, that is, carrying out an FCPA investigation within the EU can easily become quite complicated in light of the EU data protection principles and their practical application.

Despite these concerns, there may be ways to manage an FCPA investigation so as to minimize EU data protection risks. EU regulators have acknowledged **limited exceptions** to the requirement to notify persons of the processing of their

data. There are in most cases legal justifications for data processing that can be relied on other than permission from the persons whose data are implicated. Next, it's important to **be clear about the purpose of the investigation itself** − if it is to determine the truth about a certain event, then the investigatory process will be designed to ultimately produce accurate data. Pre-screening measures can be adopted to limit the data collected. Where demands of one government are contrary to the laws of another country, then judicial cooperation may provide a solution. And there are **numerous exceptions for transferring data outside the EU**. The conventional wisdom has it that transferring data outside the EU is tedious or perilous within the confines of EU laws. While in some cases that may be true, there are at a minimum risk mitigation strategies that can be adopted, such as determining the exact location of the data; transferring de-identified data; filtering data prior to transfer; and reviewing data in the EU so as to or delay or avoid or minimize transfer.

There are **very practical options too, for mitigating EU data protection law risks**. Data sources are typically varied and redundant, and risk may be minimized by taking into consideration the ease of access to data and the location of the data. There may also be a choice as to whether to rely on third parties for data harvesting or to task internal teams. Judicious use of written consents may not only be a method of lawful data collection, whether electronically or during an interview, but also a psychological balm.

When a US authority is already involved in the investigation, an open dialogue, up front, may ease the **adoption of compromise solutions** to gather data in a manner compliant with EU data protection laws. And, as noted above, in certain cases, the internal investigation may even be supplanted by cooperation between authorities of different countries, which can resolve conflicts between EU data protection laws and DoJ or SEC demands.

Finally, there is the question of mitigation of the biggest risk in an FCPA investigation − the human element. Non-cooperation by suspects or alleged wrongdoers may be flagrant or subterranean – but these individuals likely have an incentive to undermine any discovery of incriminating facts in an investigation. EU data protection laws (like the EU's labor and employment laws) may offer suspects opportunities for leverage, particularly in countries where data protection, labor and employment law violations themselves can attract criminal liability.

In sum, the type and level of risk will be unique to each investigation, depending on the persons and jurisdictions involved and the nature of the allegations, but advance preparation and proven experience will be sage guides in managing the competing demands of EU data protection laws and the FCPA.

AUTHORS

Carol A. F. Umhoefer
Partner
Miami | T: +1 305 423 8500
carol.umhoefer@dlapiper.com