Q & A Cross-Border Customer Data Transfers

Each issue, Compliance Reporter*'s Q&A column enables readers to question anonymously regulatory experts on regulation. The Q&A panelists are drawn from a pool of attorneys in private practice. If you are interested in submitting questions or serving on a panel, call* ***Mark Malyszko*** *at (212) 224-3281, fax (212) 224-3686, or e-mail mmalyszko@iinews.com. For international issues call* ***Simon Kennedy*** *at (44-20) 7303-1746, fax (44-20) 7303-1707 or e-mail: skennedy@euromoneyplc.com.*

Q: If a financial services firm within the European Union transfers customers' personal data to another firm outside the EU, who is liable for ensuring the data is used correctly?

A: Actually, it depends on how the transfer of the data has been legitimized. The transfer of personal data to any country outside of the EU is restricted by the European Data Protection Directive. Personal data should not be transferred unless there are "adequate safeguards" in place to protect the rights and freedoms of the individuals. The EU firm is liable for ensuring that the transfer can actually be made. Incidentally, the firm also needs to bear in mind that data protection law places restrictions on whether personal data can be transferred to another firm even within the EU. This answer assumes that those requirements have been fulfilled—and the only issue is whether the recipient can be outside the EU.

PANELIST
Renzo Marchini, solicitor
Dechert (London)

Some countries, including Switzerland and Canada, have what are considered by the EU to be satisfactory data protection laws, and so have been designated as always providing adequate safeguards. If data is transferred to firms in those countries, then there should generally be no liability for the EU firm. The non-EU firm will only be liable to the extent that it does not then process the personal data in accordance with its national data protection laws. For the transfer to other countries, various methods can be used to legitimise the transfer.

EU Sanctioned Model Contracts

The **European Commission** provided model contracts in 2001 whose use would constitute adequate safeguards for the transfer of personal data outside the EU. From April 1, 2005, EU firms will have the choice between two sets of mutually exclusive model contracts. The second set of standard clauses has been introduced in answer to the various criticisms of the original model contract clauses. One of the many problems of the 2001 model contracts was that it created a situation where the EU firm would itself be liable if the recipient firm did not comply with data protection rules.

The new set of standard clauses seeks to address this criticism of the 2001 version. The liability of the EU Firm here is based on "due diligence"; that is, the EU firm must have used reasonable efforts to determine the data recipient is able to satisfy its legal obligations. As long as reasonable checks are made, the sending EU firm will not be liable if the recipient does not comply.

Unfortunately, not everything is clear cut, as the rules go on to say that any individual who thinks the rules have been breached can only enforce rights directly against the recipient once the EU firm has been given a reasonable time to enforce the contract it has with the recipient. If the EU firm does not take appropriate steps to enforce the contract then the relevant data protection authority may exercise its powers to prohibit or suspend that EU firm transferring the data.

Other Ways To Legitimize The Transfer

Binding corporate rules (BCRs) constitute an internal document within a group setting out how the companies in that group intend to provide adequate safeguards to individuals whose personal data is being transferred to a third country. The BCRs need to be approved by the relevant national data protection authority. One of the requirements is that there is a company in the group within Europe that takes responsibility. Accordingly, here the EU firm is liable for the behaviour of its fellow group companies in relation to data protection.

The directive contains a number of express derogations where the restrictions on transferring personal data out of the EU will not be applicable. The most relevant of these derogations are consent of the relevant individual and where the export is necessary for contractual performance. In these cases, there is no question of the EU firm being liable for the recipient's breach of data protection rules. Where the recipient is a U.S. company, that recipient can join the U.S. "safe harbor" scheme (www.export.gov/safeharbor/) and that in itself would legitimise the transfer by the EU firm. In this case the EU firm would have no liability for breaches by the U.S. company.