THE DATA CONUNDRUM

TECHNOLOGY

Develop protocols now to comply with court data demands without breaching privacy laws.

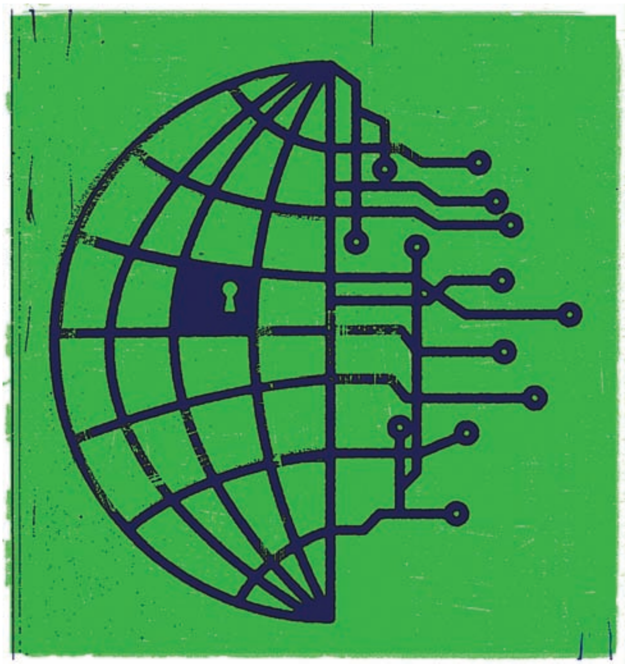
Companies operating in both the United States and the global marketplace increasingly face U.S. legal and regulatory bodies demanding employee documents from jurisdictions with strong data protection laws. If unprepared, a company can face an untenable choice — either be in contempt of a U.S. authority or face possible criminal or civil charges for contravening data privacy laws in the country where the data reside.

In 2009, Gucci America filed suit against a company, alleging it was selling counterfeit Gucci products. The United Overseas Bank found itself a third party to the suit. Its New York agent was subpoenaed to provide banking data in Malaysia, where the funds from the sales allegedly were. The bank protested, citing Malaysia's strict banking secrecy laws. Nonetheless, the courts ordered the bank to comply, confronting it with the choice of being in contempt of a U.S. court or facing criminal prosecution and nearly $1 million in fines in Malaysia.

CRAIG EARNSHAW
Managing Director, FTI Technology, FTI Consulting
craig.earnshaw@fticonsulting.com

VEERAL GOSALIA
Senior Managing Director, FTI Technology, FTI Consulting
veeral.gosalia@fticonsulting.com

ILLUSTRATIONS BY HEADS OF STATE



Dilemmas like this one are on the rise. Laws such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act cross borders. Unprepared companies face costly measures to comply and avoid penalties. The SEC, for example, can fine and even delist a company.

PERSONAL DATA CAN'T CROSS BORDERS EASILY

More than 65 countries have enacted laws to protect personal information. Specific industries are also subject to privacy regulations, such as the U.S. Health Insurance Portability and Accountability Act and the Bahamas Bank Secrecy Act. Privacy laws often prohibit exporting personal data to certain countries, in some cases even if a court subpoenas the data. The European Union, for example, allows personal data to be exported only to Argentina, Canada, Guernsey, the Isle of Man, Jersey and Switzerland, but not to the United States.

Unfortunately, U.S. authorities are often unsympathetic when companies claim that EU laws prevent them from supplying information. For example, in 2007 Credit Lyonnais was sued in the United States under the 1992 Anti-Terrorism Act. The suit alleged that the bank maintained records for a charity that was a terrorist front. The U.S. court ordered the release of account data and assumed that France wouldn't uphold its privacy laws in this case. However, French lawyers who released the data were prosecuted and convicted.

Companies with operations in both the United States and the EU must find ways to comply with both sets of laws. They might consider the U.S. Department of Commerce's Safe Harbor program, or implement binding corporate rules. They can also adapt EU-model contractual clauses.

U.S. courts and regulators may grant extra time if they are informed of countervailing laws in another country, but there are no guarantees that the other country will bend on those laws. So management must be prepared to submit the data within the bounds of EU laws. This means developing systems and processes that efficiently deal with such requests.

IF A COMPANY IS NOT PREPARED...

EU regulatory authorities may grant

permission to export personal information needed for a U.S. legal proceeding beyond the solutions described above. However, the process must be extremely well executed and must keep the information secure. The first step is to work with local counsel and establish a collection-and-review protocol for the subpoenaed information. Documents should be reviewed in a secure environment — such as a "war room" — in the country where the information resides. The data should not cross any borders.

Next, determine precisely what the investigating authority wants, then take steps to minimize the disclosure of unnecessary personal information. For example, e-mail can be culled by relevant keywords or date ranges, and attorneys can pull out only relevant information from the remaining e-mails. If these steps are followed, it is much more likely that the local authorities will grant permission to export the data.

AVOID THE COSTS OF BEING UNPREPARED

Once a company understands the data privacy laws in each country where it does business, it can develop a strategy to provide subpoenaed information with far fewer headaches.

However, compliance can affect numerous operational decisions. For example, many jurisdictions outside the United States require a company to know where employee data are physically located. But today, cloud computing applications can aggregate and move data across borders.

Companies should regularly re-examine and update document retention and storage policies to reduce the burden of restoring and recovering data from legacy systems and archives. Management must also know the location of data that might be needed in future disputes or investigations.

Finally, companies should be prepared in advance to structure information with appropriate protocols to facilitate in-country review and expedite permission to export. Also, employment contracts could include clauses that grant rights to transfer personal information in response to legal requests and issues. Companies can utilize other mechanisms, such as Safe Harbor schemes and binding corporate rules, to expedite the transfer of data outside the EU.

> Companies with operations in both the United States and the EU must find ways to comply with both sets of laws.

The growth of national and industry efforts to protect private information can easily land companies between a rock and a hard place. However, the difficult choice between violating laws in one jurisdiction and being in contempt of a regulatory body in another can be averted. To do so, management should seek to develop structures and protocols that allow it to comply with the laws in each country where it does business. For companies that have not yet done so, now is not too soon to start. ■

The views expressed in this article are those of the authors and not necessarily those of FTI Consulting, Inc., or its other professionals.