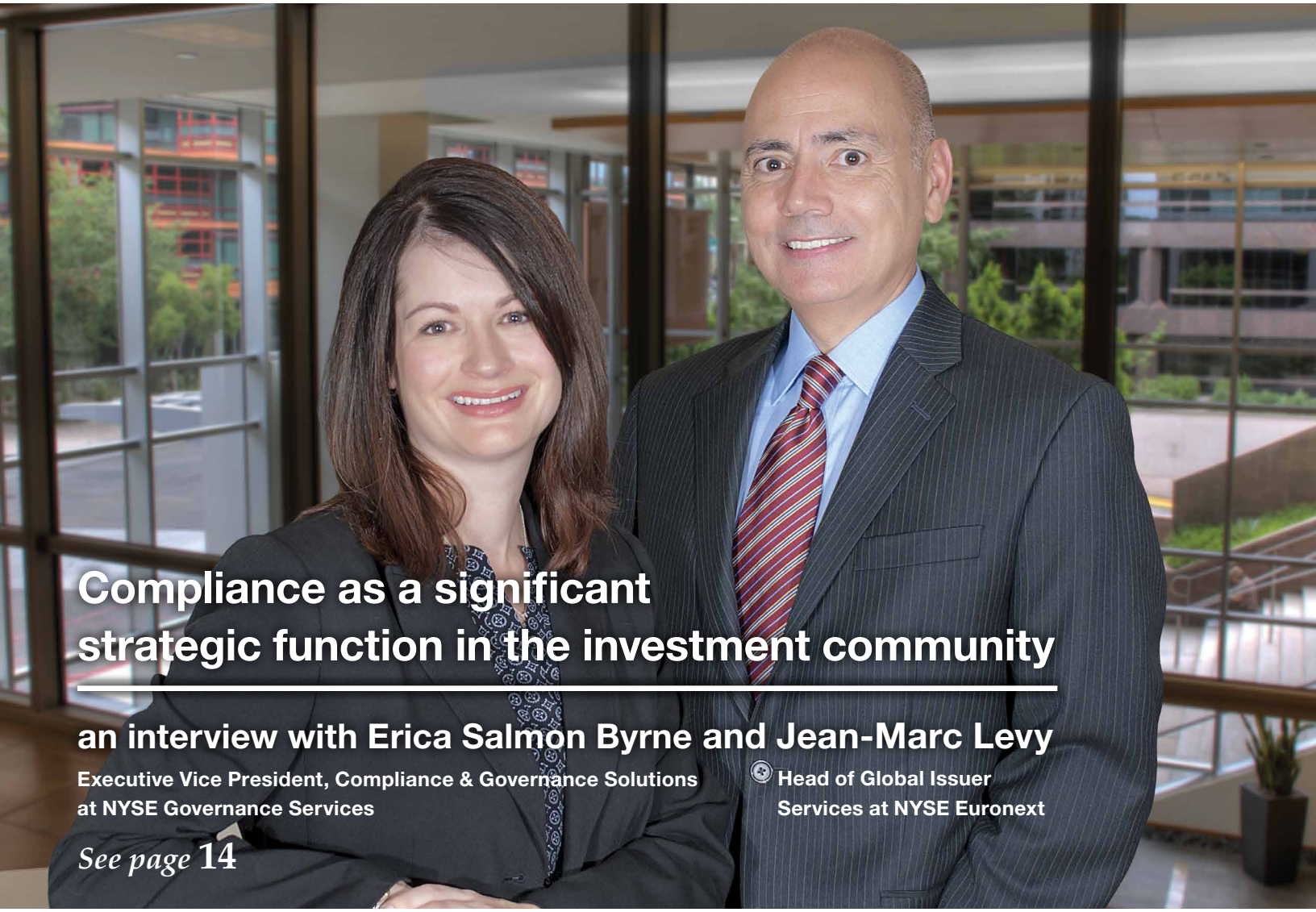
Compliance & Ethics Professional

November/December 2013

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org



Compliance as a significant strategic function in the investment community

an interview with Erica Salmon Byrne and Jean-Marc Levy

Executive Vice President, Compliance & Governance Solutions at NYSE Governance Services

Head of Global Issuer Services at NYSE Euronext

See page 14

By Kristy Grant-Hart, JD, CCEP-I

New European law will change everything you do with data

» Current European data protection laws are different in each country.
» The proposed regulation will apply uniformly to all European countries.
» European citizen's data protection rights will follow them everywhere they live.
» Businesses should overhaul their data protection programs to comply with the draft regulation.
» Direct consent will be required for all marketing to customers or sale of customer data.

Confusion—that's the most common response the first time a non–European-based compliance professional comes across the myriad data protection and privacy laws in the European Union. Why can't a company simply collect a German employee's email for review in the United States without obtaining the employee's consent? Why does a company have to involve the French works council (or union) if it receives a whistleblower hotline report about a French manager? Thus far, complicated European Union (EU) laws on data protection haven't applied outside of Europe. Multi-national companies frequently have compliance procedures relating to data protection and retention that differ for the EU countries and the rest of the world. That is about to change.


Grant-Hart

The current law in the European Union

The data privacy and protection laws in the EU are all based on the European Union's Directive 95/46/EC, commonly referred to as the "Directive."[1] This law, enacted in 1995, was meant to create a singular standard to which each European country would comply. The Directive ordered the various EU governments to implement the law in their local legislatures. The problem is, each legislature interpreted the law in a different way. Some countries, like France, implemented the Directive with force, creating a complicated and strict system of filings and rules. Other countries, like the United Kingdom, created a version of the law that is much more relaxed.

This inconsistent legislation has led to the situation today, where in Germany, the works council must approve a company's whistleblower hotline before it can be implemented, but in Italy, no consultation with the works council is required.

The Directive was created when the Internet wasn't yet in popular use for businesses. The current law creates huge expense, with companies forced to file with multiple data protection authorities to note their various data processing activities. The proposed European regulation could change all of that.[2]

The proposed regulation

In 2012 the European Commission proposed a draft law meant to take the place of the old Directive. The new law is not a directive, but instead a regulation. The new law (draft regulation) would be immediately binding on *all* European countries, in the form that it is written. It would not be up to the countries to interpret the law and to implement it in their local legislature. Instead the new draft regulation would be effective throughout Europe in one form.

The draft regulation is currently being hotly debated. Over 4,000 amendments have been proposed, and US companies from Google to Apple are pouring hundreds of thousands of dollars into lobbying efforts to change the law before it is passed, which is expected to be in 2014.[3]

Over 4,000 amendments have been proposed, and US companies from Google to Apple are pouring hundreds of thousands of dollars into lobbying efforts to change the law before it is passed, which is expected to be in 2014.

Why the regulation would apply worldwide

The current Directive only applies to data processed within Europe. Therefore, for example, if a company has a data breach, the first question is, "In which country did this happen?" If the data breach occurred in Alabama and relates only to an Austrian citizen living in Alabama, there is no need to tell the Austrian data protection authority, or notify the impacted Austrian citizen of the breach.

The draft regulation would change this, because the rights of EU citizens would travel with them all over the world. Therefore, if a company has a serious data breach, and it affects an Austrian living in Alabama, the company will have to tell the Austrian data protection authority and the Austrian, because the right to know about the breach is carried by the Austrian wherever he/she goes, as a right, based on the law.

The effect of this provision cannot be overstated. In effect, the EU draft regulation would necessarily affect all companies that collect or process data all over the world, because there are citizens of the EU in most or all countries in the world. It will no longer matter that a business is purely based in a country outside the EU. If the business services citizens of the EU, it would be required to comply with the new regulation.

Much bigger penalties

The draft regulation comes with much bigger penalties than the old country-based laws. Currently, each EU country's data protection authority can impose monetary penalties, but the draft regulation ups the ante, allowing for penalties up to one million Euros or 2% of the companies' global annual turnover for serious data breaches.

New challenges for companies – New rights for citizens

The draft regulation imposes some interesting new "rights" for citizens, with corresponding challenges for businesses. Two of the more interesting rights are the right to be forgotten and the right of data portability.

The right to be forgotten allows people to ask that their data be deleted if they no longer want it to be processed, and there is no legitimate reason to keep it. The question remains

of course, is this even possible? People can download items from the Internet on their computers, and cache websites, even when the information has been deleted from the original source. The right to be forgotten will impose requirements on business to implement measures for individual data deletion that are more cumbersome and costly than exist today.

Internet-based companies may be concerned about the right to data portability. This right allows any person to request that a copy of all of his/her electronic data be transferred to another provider or service. The implementation and feasibility of this provision is currently under review. If a person changes email providers, does the former provider have to provide a copy of all of the previous email from the past five years? The logistics of this provision have not been tested or explained.

The good news for compliance professionals is that the draft regulation requires that all companies that employ more than 250 people must designate a data protection officer.

Requirement of explicit consent

Perhaps the provision of the draft regulation that will most affect businesses is the requirement of explicit consent from a person to process his/her personal data. "Processing" includes things like marketing messages and product suggestions, as well as the sale of member lists, email addresses, and other consumer information. Under the draft regulation, a person would have to specifically give permission to a company to allow this activity, undermining financial models based on the collection, sale, and use of personal data for marketing purposes. Additionally, under the draft regulation, people would have the right to withdraw their consent at any time.

The requirement for explicit consent for the use of personal data applies to *any* use of a person's data that is not strictly required for the completion of a contract or service requested or paid for by the customer. Any communication or marketing outside the initial service would need to be explicitly consented to or a fine could be levied on the company. Additionally, the consent of the person loses its effect once the initial purpose for which the data was collected is complete. In other words, once a company's service has been rendered, explicit consent from its customers would be required to continue to email them offers or information about the company's new services, or to present them with a customer satisfaction survey.

Wanted: Company data protection officers

The good news for compliance professionals is that the draft regulation requires that all companies that employ more than 250 people must designate a data protection officer. This requirement is based on the German model, which ensures that each company has an in-house expert monitoring the data processing activities of the company. It is unclear from the law, as currently drafted, whether this person would need to be employed exclusively as a data protection officer or whether the role could be part of a compliance or IT specialist's duties. It is also unclear whether it would be possible to impose this obligation on

companies operating outside the EU that do business within the EU.

Data breach notification

Currently, only a few EU countries require notification of a serious data breach to the country's data protection authority or to the affected people. This too may change, as the draft regulation states that companies must notify the data protection authority and data subjects of a serious data breach as soon as possible. The draft regulation envisions a 24-hour notification period, which many experts believe to be an unreasonably short timeframe.

What's next?

The European Parliament-Council plans to negotiate a final version of the regulation during the latter part of 2013. By the beginning of 2014, the Civil Liberties Committee is slated to vote on the text approved by the Council, then the entire Parliament will vote on the final form of the law. The finalized law should enter into force in 2014, but will likely not become enforceable by fine and penalty until 2016. Two to three years may sound like a long time, but given the vast changes required in most companies for compliance with all of the aspects of the law, compliance professionals should monitor developments and begin initial preparations and planning immediately. ✳

Kristy Grant-Hart *(kgrant-hart@carlsonwagonlit.com) is the Director of Compliance for Europe, the Middle East, and Africa for Carlson Wagonlit Travel in London.*

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal L 281, Nov. 23, 1995. Available at http://bit.ly/1bndMSj
2. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on free movement of such data (General Data Protection Regulation), Jan. 25, 2012. Available at http://bit.ly/19RO7za
3. Kevin J. O'Brien: "Firms Brace for New European Data Privacy Law." *New York Times* online. May 13, 2013. Available at http://nyti.ms/18Hl6b5