



Privacy & Information Security Update

January 2012

European Commission Proposes Sweeping Changes to Data Privacy Regulation

Since the mid-1990s, the European Union and its member states have enforced one of the most stringent privacy and data security regimes in the world. Because so many businesses now compete in global markets and are increasingly integrated into cross-border commerce, European privacy rules both directly impact companies' international operations and have become de facto standards in many industries. Changes in European privacy laws inevitably impact domestic U.S. business practices, now more than ever.

Carrying this trend into new territory, the European Commission (EC) on January 25, 2012 proposed a comprehensive revision to its data protection rules. The new proposed privacy directive is based on the EC's stated goal of increasing the control individuals may exercise over their personal information, even information they previously disclosed or publicly used. The new directive also seeks to simplify and harmonize the national treatment of data privacy among the EU member states. A vote is expected in the European Parliament by the end of 2012, resulting in the expected enactment and enforcement of a new Data Protection Framework beginning sometime in 2013.

While the 119-page document contains myriad new obligations and procedures, a few of them will have immediate and substantial impact on both U.S. and international businesses. These include:

- **Scope of Jurisdiction** – The scope of the new regulation is extended to apply to entities located anywhere in the world that process the personal data of EU residents, substantially expanding the effective reach of the directive.
- **Heavy Sanctions for Non-Compliance** – Organizations will be exposed to monetary sanctions of up to €1 million or up to 2 percent of their global revenues.
- **Explicit Consent** – The new regulation enhances the standard for measuring whether an employee, customer, or other person consents to the use or disclosure of their personal information. This will require more explicit and detailed disclosures and express consents.
- **Compelled Disclosure of Data Breaches** – The new directive introduces a data breach notification requirement, something already familiar to U.S. businesses but which now adds new European obligations to those already faced by domestic businesses if the data of European citizens are breached. The new directive would impose very short deadlines for notification in some circumstances.
- **Impact Assessment** – Businesses now will be obligated to conduct data protection impact assessments prior to engaging in certain “risky” data processing operations.
- **Data Protection Officers** – The regulation requires that companies with more than 250 employees or those whose “core activities” relate to data processing designate data protection officers. Companies meeting the 250-employee threshold that are not located within the EU but that process personal data of EU residents will be required to designate data protection representatives in the EU.
- **Cross-Border Data Transfers** – Transfers of data outside the EU will still be permitted where adequate protection is established. Transfers can

be made for the company's legitimate interest so long as these transfers are not frequent, massive or structured, and adequate security safeguards are in place. The proposed directive leaves in place the "Safe Harbor" framework many domestic companies use to transfer European data to the United States.

- **Right To Be Forgotten and Erasure** – The new directive recognizes a novel (and, to many businesses, counterintuitive) "right to be forgotten," which enables individuals to require a company with which they have done business to erase and cease using information previously provided by the individual.

The new directive will have substantial and lasting impact on the information practices of many businesses, and the time for planning a compliance strategy will come well before the actual effective date of the new directive. Thompson Hine's globally recognized Privacy and Data Security Team is ready and able to assist you in your own privacy and data security assessment and planning.

FOR MORE INFORMATION

For more information, please contact:

Thomas F. Zych

216.566.5605

Tom.Zych@ThompsonHine.com

Michelle W. Cohen

202.263.4151

Michelle.Cohen@ThompsonHine.com

Darcy M. Brosky

216.566.5774

Darcy.Brosky@ThompsonHine.com

Christopher M. Comiskey

216.566.5658

Christopher.Comiskey@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgement of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2012 THOMPSON HINE LLP. ALL RIGHTS RESERVED.