BNA

Privacy and Security Law Report®

EU Data Protection Framework

An unofficially released draft of a new EU-wide regulation to replace the 16-year-old EU Data Protection Directive would have a significant impact on global businesses by introducing further complex restrictions on global flows of personal data, significant internal compliance requirements, and fines that range up to 5 percent of a company's *global* gross revenue, Sidley Austin LLP attorneys write.

First Look: Leaked Draft of New EU Data Protection Regulation Suggests Significant Impacts for Global Businesses




By Alan Charles Raul, John Casanova, Edward R. McNicholas, and William R.M. Long

Alan Charles Raul, John Casanova and Edward R. McNicholas are global coordinators of Sidley Austin LLP's Privacy, Data Security and Information Law group. Casanova is based in Sidley's London office, along with William R.M. Long, who is a member of the group. Raul and McNicholas are based in Washington. The views expressed herein are those of the authors personally and do not necessarily reflect the views of any governmental or private entity, client, or association. This article is published for informational purposes only and is not legal advice.

A draft of a new EU-wide regulation to replace the existing EU Data Protection Directive has been unofficially released. The draft ''General Data Protection Regulation,'' which is due for official publication in January 2012, will have a significant impact on global businesses by introducing further complex restrictions on global flows of personal data, significant internal compliance requirements, and fines that range up to 5 percent of *global* turnover/gross revenue. That is, potential fines under the new EU law could range into the hundreds of millions of Euros. The current draft, however, will likely evolve due to expected lengthy negotiations as the draft moves through the EU's legislative process. Nonetheless, some version of the new Regulation is projected to be approved, at the earliest, in 2014. Significantly, while the existing Data Protection Directive was not self-executing—each Member State had to implement the Directive's basic framework in its own

 ISSN 1538-3423

national law—the new Regulation would itself be binding throughout the European Union following enactment by the Council and Parliament of the European Union.

Given the breadth of proposed changes in the EU data protection regime, companies with EU operations, employees or customers should monitor the ongoing evolution of the draft Regulation. Numerous opportunities to influence the ultimate form of the Regulation will be available during the next two years. In addition, because of the potentially significant impacts on international trade in information services and data flows, businesses may wish to consult with the relevant EU and U.S. government agencies in order to express their concerns and advocate their interests.

The original Directive was adopted in 1995—before the advent of the commercial web and use of public and private ''Clouds.'' Accordingly, revision of the prior Directive has been contemplated for some time to take account of the increased collection and international sharing of globalized data that have brought new challenges for the protection of privacy. As the new Regulation would be directly applicable throughout the European Union, the revision may help facilitate the free flow of data among the Member States by forging a single data protection law that avoids the differences that currently exist among Member States' national data protection laws.

The new Regulation would apply to businesses even if they are not ''established'' in the European Union and do not use equipment located there.

While global business may applaud the goal of providing a more harmonized and consistent set of EU data protection rules, the new Regulation would retain many of the existing restrictions on data use and collection, including certain prohibitions on international data transfers, while adding significant new regulatory requirements. New requirements would include obligations relating to documentation of processing, appointment of data protection officers, and the duty to conduct data protection impact assessments.

Many of the developments in this complex draft were foreshadowed in prior Article 29 Working Party analysis, but some of the most striking aspects of the draft Regulation bear particular mention.

Extraterritorial Application to Non-EU Businesses: The new Regulation purports to regulate any businesses that ''direct'' processing activities with respect to individuals in the European Union. In other words, the new Regulation would apply to businesses even if they are not ''established'' in the European Union and do not use equipment located there. This would have important implications for non-EU based businesses that have EU customers. For example, the Regulation would potentially apply to a California web-based company with offices only in California but operating a website that is accessible around the world and does business or otherwise interacts with customers in the EU.

Increased Enforcement and Penalties: Significantly, the draft Regulation includes potentially enormous penalties of up to 5 percent of the annual worldwide turnover (gross revenue) of a business that fails to comply with the Regulation. To date, enforcement of the current Directive has varied significantly among the different Member States, and potential fines have been relatively minimal in some countries. The new Regulation would empower supervisory authorities to impose a temporary or definitive ban on processing, suspend international data transfers, and enter premises and impose fines for criminal offenses. Individuals would also have the ability to lodge a complaint with any supervisory authority in any Member State, either as individuals or as a class. This recognition of ''class'' action is obviously a significant potential change, given that such lawsuits are now rarely filed in the EU.

Accountability: Data controllers would be required to adopt policies and implement appropriate measures to ensure, and be able to demonstrate, that the processing of personal data is performed in compliance with the data protection principles and other requirements in the Regulation, including the mandatory training of staff. In addition, both data controllers and data processors would be required to keep a potentially exceptionally burdensome record of all forms of processing of personal data by the business, often called a ''data map.''

Moreover, the Regulation includes a generalized requirement to use so-called ''privacy by design'' elements. That is, data controllers must implement mechanisms to ensure that only the minimum personal data that are necessary for each purpose are collected and retained. This would likely result in increasing use of data protection audits and significant internal compliance costs, and may inhibit innovations in future uses of data and development of new products or services.

Privacy Impact Assessment: The new requirement to conduct privacy impact assessments (''PIAs'') will be very significant. In particular, the new Regulation provides that ''[p]rior to the processing of personal data, the controller or the processor shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where those processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.'' *This written assessment would require consultation with data subjects and would be made public.*

Privacy Policies and Notifications: The existing technical requirement under current data protection laws in some EU Member States to provide notice of certain forms of data processing to a local Data Protection Authority will largely be abolished. Under the draft Regulation, a data controller would be obliged to consult a supervisory authority where a data protection impact assessment shows that processing is likely to present a high degree of risk, for example processing of health data.

Lead Authority: In a positive move for harmonization, a ''lead authority'' would be designated where a data controller is established in more than one Member State based on the presence of its ''main establishment.''

Codes of Conduct: Use of codes of conduct and certification schemes, such as data protection seals and marks, would also be encouraged so that individuals could assess the level of data protection applied by a business.

  PVLR ISSN 1538-3423

Further Limitation on Use of Consent: The Regulation would significantly restrict reliance on consent ''where there is a significant imbalance in the form of dependence between the position of the data subject and the controller.'' And in a particularly significant blow to the rights of employers, ''Consent shall not provide a legal basis for the processing . . . for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law.'' This rule would make the most restrictive views of employee consent the rule across the EU.

Further International eDiscovery Complications: In a clause that will surely provoke and complicate compliance with U.S. legal process by international companies, the new Regulation would provide that ''No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner,'' unless allowed under separate international obligations, e.g., the Hague Convention. Instead of complying with U.S. legal process for EU personal data directly, data controllers would be required to inform and obtain prior authorization from the relevant DPA. This situation would become all the more complicated because there is also a proposal for a new Police and Criminal Justice Data Protection Directive as well as an exemption from the Regulation for any matters concerning ''national security.'' This segregated authorization process will put global businesses directly in the middle of the long-standing discovery differences between the U.S. and EU, particularly if the DPAs continue their interest in pursuing matters, such as the SWIFT case, in which personal data in the hands of a global corporate entity is ordered to be produced for national security and international law enforcement purposes. This raises concerns whether the new Regulation could function as a quasi-blocking statute from a U.S. perspective.

Data Protection Officers: The draft Regulation also adopts an existing requirement from Germany, making it mandatory to appoint a data protection officer for the public sector and in the private sector for large enterprises (over 250 employees) or where the organization's activities include regular and systematic monitoring of individuals. The Data Protection Officer would have various duties to ensure compliance and would have a term of at least two years. The supervisory authority and the public would have to be notified of the Officer's appointment.

Increased Rights of Data Subjects, Including ''Right to Be Forgotten'': The draft Regulation also introduces the obligation for the data controller to have transparent and easily accessible data protection policies and provide information using clear and plain language. A data subject would also have a right to correct his or her personal data and, importantly for social media, a right to be forgotten (i.e., to have his or her data erased) and a right to data portability (i.e., to transfer their personal data to another provider). Significantly, although the Regulation notes, but does not resolve, the tension between principles such as a ''right to be forgotten'' and principles of freedom of expression, or, as one might say, a ''right to remember.''

Data Security: The proposed Regulation would require both data controllers and data processors to implement appropriate technical and organizational security measures following an evaluation of the risks. As under the existing regime, a data controller will be required to choose a data processor that provides guarantees as to its security measures and must have an agreement with a data processor. In the event of a security breach, the data controller must, without undue delay, inform the supervisory authority and, where the breach is likely to adversely affect a data subject, inform the data subject. In either case, as a rule, notification is required within 24 hours.

Transfer of Personal Data to Third Countries: Where personal data are to be transferred to countries outside the European Union that are not considered by the European Commission to provide an adequate level of protection, two main solutions could be used by a data controller or a data processor to permit the transfer: (i) use of Binding Corporate Rules (''BCRs'') which must comply with specified requirements and be binding on the business; or (ii) use of standard data protection clauses adopted by the Commission. The lead supervisory authority for the data controller would approve these BCRs, and there has certainly been renewed enthusiasm for widespread adoption and rapid and harmonized approval of BCRs. Nevertheless, it is assumed that the current U.S.-EU Safe Harbor would also remain in place as another way to legitimate the adequacy of international data transfers from the EU to the United States. Significantly, the new Regulation contemplates that specific sectors of a country could be deemed adequate—perhaps paving the way for recognition of the U.S. health, communications, and financial sectors.

The new Regulation contemplates that specific sectors could be deemed adequate—perhaps paving the way for recognition of the U.S. health, communications, and financial sectors.

European Data Protection Board: A new European Data Protection Board would be created to replace the existing Article 29 Working Party and help ensure consistent application of the new Regulation. The Board would consist of the heads of the supervisory authority of each Member State and the European Data Protection Supervisor, and it would have more robust powers than the existing Article 29 Working Party.

The draft Regulation may be revised before it is officially published as a draft proposal by the European Commission at the end of January, and it will no doubt be subject to lengthy and robust discussion and revision before it is finally adopted and becomes law. What is crystal clear, however, is that, whatever the final form of the Regulation, it will have a significant impact on essentially all businesses with European customers, employees or operations within the European Union.

Given the likely new policy developments in the United States on privacy to be emanating shortly from the Commerce Department and Federal Trade Commission—and perhaps Congress as well—companies should actively monitor how the new approaches to data protection in Brussels and Washington will affect their businesses and practices. There will

also be considerable opportunity to participate in the policy making process in both the EU and the United States for companies with a particularly strong interest in being heard. The impacts on international trade in information services and the free of flow of data across the Atlantic may also be significant enough to warrant bilateral discussion by the trade representatives of the United States and European Union.

Full text of the 116-page ''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 the free movement of such data (General Data Protection Regulation) (Text with EEA [European Economic Area] relevance) Version 56 (29/11/2011)'' is available at http://op.bna.com/pl.nsf/r?Open=dapn-8pbkkb.

  PVLR ISSN 1538-3423