Viviane Reding, the European Commission vice-president and justice commissioner, launched a proposal on January 25, 2012, for a new EU Data Protection Regulation, referred to as the “General Data Protection Regulation” (GDPR). If adopted, the GDPR would reshape the European data protection framework in a harmonious way, ensuring EU residents a high level of protection for their personal data. Already, this European Commission proposal has elicited much attention in the legal and business world. After putting the GDPR in perspective, this article will:

Briefly discuss legislative action and the time frame, set out some important (and sometimes controversial) provisions, and attempt to draw lessons for businesses.

**The GDPR in Perspective**

The proposed GDPR arises in a context where the protection of personal data in a constantly (and rapidly) evolving technological context is a concern on both sides of the Atlantic. One manifestation of this concern is the High Level Conference on Privacy and Protection of Personal Data held simultaneously in Washington and Brussels, which led to a joint statement on March 19, 2012, by Viviane Reding and former U.S. Secretary of Commerce John Bryson, emphasizing the need for more interoperability of European and U.S. privacy systems “on a high level of protection.”

**A Need for Greater Uniformity in EU Law**

The choice of a regulation as the EU legislative instrument to achieve such a high level of protection was made because regulations become law in the same form in all of the current 27 Member States of the EU and in new Member States, thereby promoting uniformity of law in the EU, which contrasts with the differing ways in which the current Data Protection Directive (Council Directive 95/46) (the “Directive”), which was adopted in 1995, was subsequently implemented (or “transposed”) by national law in the various EU Member States. This divergence in implementation occurred in spite of compliance with the required minimum standards of the Directive.

Such divergence was made possible because, according to Article 288 of the Treaty on the Functioning of the European Union, as in force today, it is left up to the “national authorities” of the Member States to choose the “form and methods” of the implementation of directives. For example, France may act to implement a directive by the method of adoption of a bill in the French parliament or by a presidential decree, when the French president is so empowered. Likewise, Spain, within some limits, may choose a different form for the instrument by which it implements a directive than that chosen by France, so long as the result to be achieved is so achieved.

Now, multiply this situation by each of the 27 Member States to which the directive is addressed, and you can see how a possible result is divergence.

**The Potential Positive Effects of Increased Trust**

One of the objectives of the European Commission in proposing the GDPR is to increase trust in the use of information services by EU users, while protecting their fundamental rights. It is thought that increased trust should encourage a further development of information services in the EU, furthering its digital agenda and providing economic advantages to companies, such as increased sales, and to the European economy, through additional growth and greater employment. Neelie Kroes, EU digital agenda commissioner, recently highlighted the importance of trust (or lack of distrust) in the establishment of “new and bigger markets.”
New Technology Leads to New Challenges to Privacy
The area of data protection is one in which Europe has much experience both at the Member State level (for example, France had a statute as early as 1978), and at the EU level (the Directive, followed by over 10 years of application). One may also highlight in passing the difference in the European “global” approach to privacy and personal data protection and the U.S. “piecemeal” approach, with legislation crafted for specific sectors or issues. Nonetheless, because of the technological advances realized in the ensuing years and unforeseen in 1995, such as biometrics, facial recognition software, increased data storage capacities, cloud computing systems, and social networks, more personal data (and more intimate personal data, in all senses of the term) are collected and processed. This has resulted in new challenges to privacy, which has led the European Commission to propose the replacement of the Directive with a new data protection framework, including the GDPR.

Legislative Action and the Time Frame
Although today it is uncertain whether or not the GDPR will be adopted and, if adopted within which time frame, we already have some indications as to the preliminary legislative action and certain elements of the potential time frame. For example, a tentative calendar for the GDPR published in May 2012 by its rapporteur in the European Parliament foresees the GDPR coming to a vote before that legislative body in early 2014.

The European Parliament
The LIBE (Civil Liberties, Justice and Home Affairs) Committee of the European Parliament has been appointed as the main committee with responsibility for the GDPR, although other committees are involved, i.e., Internal Market and Consumer Protection (IMCO), Industry, Research and Energy (ITRE), Economic and Monetary Affairs (ECON), Legal Affairs (JURI), and Employment and Social Affairs (EMPL), possibly indicating that the parliament considers the fundamental rights elements of the GDPR of greater importance than the economic ones, while acknowledging that economic elements are present. Recently, a meeting on the proposed data protection reform was organized with members of national parliaments, and the LIBE Committee should also be presenting a draft report on the data protection reform by the end of 2012.

The Council of the European Union
However, the European Parliament and the European Commission are not the only EU institutions involved in the data protection reform process. The Council of the European Union (EU Council), through its working parties, is also reviewing the proposed GDPR and is discussing amendments to it. The EU Council’s Working Party on Data Protection and Exchange of Information (DAPIX) has suggested proposed changes to certain articles of the GDPR. In addition, there are divergent views in various Member States on several provisions of the GDPR, and even as to the choice of a regulation as the appropriate legislative instrument. One element of the GDPR that has also been criticized is the Commission’s role to act through delegated and implementing acts (for example, enabling of the Commission to adopt delegated acts to specify criteria and conditions and for processing special categories of personal data), as this might be considered to give the Commission too much discretion in defining the application of the GDPR.

Council/Parliament Interface and Entry into Force
Earlier this year, a EU Council spokesman indicated that negotiations between the EU Council and the European Parliament on the text of the GDPR should begin at the end of 2012. Agreement between those two institutions on the text of the GDPR in two successive readings is required for it to become binding and directly applicable in Member States. The GDPR’s entry into force would occur 20 days after publication in the Official Journal of the European Union, however in the current proposal, it would only apply two years after such date (this time frame, however, is indicated between brackets and in italics, suggesting that it is a point open for discussion). To be clear, with the information available today, the start of the application of the GDPR (if adopted) should be expected to occur sometime during the period of 2014–2016, absent unforeseen blockages such as those which occurred during the adoption of a famous recent EU regulation in another field – REACH (chemicals and the environment).

Some Important Provisions of the GDPR
Effect on Non-EU Companies
In its current form, the GDPR would apply to controllers of personal data not established in the EU, so long as they process EU residents’ personal data related to the offer of goods or services in the EU or to behavioral monitoring. (A “controller” would include a company that collects and processes its customers’ information; for example, a company that has a customer relationship management program.) Viviane Reding has been firm on this point, but it remains to be seen whether future EU–U.S. discussions will cover this issue under the GDPR, as was done under the Directive when the 2000 Safe Harbor for transatlantic data transfers was negotiated. (It should be noted that the GDPR also contains provisions on cross-border data flows.)

Greater Uniformity of EU Law
Through its unifying effect on EU data protection law, the proposed GDPR would allow businesses operating in various EU Member States greater visibility and legal certainty in the field. (However, the delegated authority discretion of the
European Commission has the opposite effect.) In addition, the proposal for the GDPR provides that where a personal data controller or processor is established in two or more Member States, the EU Member State data protection authority of the place where the controller or processor has its main establishment would be able to supervise the activities of the controller or processor in all Member States. For example, if a company that controls or processes EU residents’ personal data has its main European establishment in Ireland, it would be able to be supervised by the Irish data protection authority, and complete EU administrative filings and formalities there for all of the EU Member States in which it operates. This is the GDPR’s “one-stop shop” provision that is designed to ease administrative formalities for some businesses, saving them time and money. Furthermore, a mechanism to ensure consistency in the application of the GDPR throughout the EU would be established.

On October 5, 2012, the Article 29 Working Party (WP29) – an independent advisory panel providing interpretative guidance on privacy directives to Member States – issued a second opinion on the data protection reform discussions and highlighted areas for “further debate and clarification” identified by the LIBE Committee of the European Parliament such as, among others, the attribution of roles in cross border cases between the various data protection supervisory authorities.

Delegated and Implementing Acts
WP29 included on the LIBE list of areas for additional work the role of the Commission to act through adopting “delegated and implementing acts.” As the WP29 opinion makes clear, these delegated and implementing acts have been made possible by the Lisbon Treaty and are based on, respectively, Article 290 and Article 291 of the Treaty on the Functioning of the European Union. Delegated acts may be used to supplement or amend the GDPR for non-essential elements. Implementing acts may be used to ensure uniform implementation of acts throughout the EU. The EU Council and the Parliament have a two-month period during which they may object and block entry into force of delegated acts.

WP29 is concerned that enabling the European Commission in the GDPR to adopt delegated and implementing acts from the start (and broadly, as this possibility is offered in many articles of the proposed legislation), without the need for making a determination of their necessity on a case-by-case basis, there is a lack of legal certainty, with the Commission being given broad discretion, which in many cases, could be handled alternatively (e.g., by interpretative guidance, through national law, or detailed in the GDPR itself).

Broad Definition of “Personal Data”
By contrast, WP29 defends the GDPR against criticism of its broad definition of “personal data,” as this is considered necessary in order to “future-proof” the proposed regulation in the context of rapid technological change. Under the GDPR, any information related to a natural person who can be identified by ways likely to be used by the controller would be caught under the definition.

By contrast, in Article 2(a) of the Directive, “personal data” is defined with respect to a person who is or can be directly or indirectly identified, particularly by “reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” Thus, the GDPR allows for the possibility of technological advances leading a controller to identify an individual through other sorts of data, which would then be protected as “personal data” under the GDPR.

Data Protection Impact Assessments
Data processing that presents “specific risks,” such as that which involves certain sensitive information (e.g., health, race, ethnic origins, sex life, etc.), triggers the GDPR requirement for a data protection impact assessment. This assessment, which must describe the processing foreseen, shall assess risks to data subject rights and freedoms, means of addressing these and those designed to protect personal data, and demonstrate compliance with the GDPR. The views of data subjects on the processing must also be sought. The data protection impact assessment is to be accomplished by or on behalf of the controller (thus, at its expense), and the Commission may adopt further criteria by delegated acts.

Data Protection Officers
Where data are processed by enterprises with more than 250 employees, under the proposed GDPR the controller and the processor must appoint a data protection officer (DPO) who has expert knowledge on data protection law. This DPO may be an employee or an independent service contractor. Concern has been expressed that this may create a great administrative burden on the smaller of these companies, which could be described as SMEs, and that other factors, such as the degree of risk related to the processing activity, should be considered before placing ad-
ministrative burdens on such companies, instead of basing this requirement on the number of employees in the enterprise.

Data Portability and the Right to Be Forgotten
Two new rights introduced in the GDPR are data portability and a general right to be forgotten. In the first of these two, data controllers must provide a data subject’s data to him or her in a format that allows transmission into another data processing system, making them “portable.” In the second, a data subject may require that all of his or her data be erased under certain circumstances, such as when he or she decides to revoke consent to processing.

Increased Fines
Fines for data protection violations by one of the most famous targets of data protection authorities in Europe – Google, for its Street View service – ranged from €100,000 to €1,000,000 in certain EU jurisdictions in 2011. If the GDPR is adopted in its current form, fines for data protection violations could rise significantly, as the proposed legislation provides for a sliding scale of fines, depending on the seriousness of the offense, whether it is a repeat offense and intentional, and whether the violator is an enterprise or not. For an enterprise, sanctions may involve a simple warning for a first non-intentional offense by an enterprise of less than 250 employees only engaging in processing as an ancillary activity, to a non-intentional offense by an enterprise or not. For an enterprise, sanctions, on the one hand, and to increase trust and improve reputation, on the other. What follows is an attempt to elucidate some of these lessons.

1. Put the GDPR on Your Radar
Becoming familiar with the GDPR and follow its development. Whether or not the provisions of the GDPR are adopted in their current form, many of the issues covered will not go away. Reform is needed. Becoming familiar with the issues now, and following the genesis of the future regulation will allow companies better to prepare for the final legislation. Legal monitoring may be considered part of good corporate legal strategy and even a necessity in today’s competitive business world, and for the international firm, EU data protection legislation is no exception to the rule.

2. Audit Risks for Potential Data Protection Violations
Companies should try to identify areas where potential data protection violations may occur, through auditing risk areas (for example, procedures for handling consent) – and may consider having this done by outside specialists. The results of these audits will allow them to identify and take measures to prevent such violations from happening. This certainly involves compliance programs.

3. Incorporate Data Protection into Compliance Programs
Another lesson to be learned is to be proactive and, if has not already been achieved, incorporate data protection into compliance programs. The potential risks for non-compliance under the terms of the proposed GDPR are great in terms of potential financial risks, but also in terms of loss of customer trust and harm to reputation. Preventing these risks through adopting adequate procedures and increasing internal knowledge through training (seminars and other means meant to raise awareness) are crucial. Follow-up of compliance efforts should be performed. This method of being proactive may make a company more competitive than its counterparts who “put out fires” instead.

4. Make Sure Proper Consent is Obtained
Where consent is required, it should be explicit, verifiable, and informed, and it should be obtained from data subjects prior to processing their personal data. The proposed GDPR places the burden of proof for this on the controller. Privacy policies should be reviewed in this light. Adequate procedures allowing for the data subject to revoke their consent should also be provided for.

5. Incorporate Privacy by Design
An additional way of being proactive is by building privacy into the technology and organization and by ensuring a high level of data security by design. Companies may reduce potential risks related to data security breaches and privacy violations in this way.

6. Prepare for Data Breaches
No one wants a data breach; however, with new rules as to notification of data breaches, developing the means of identifying them, and communicating about them rapidly – including between the controller and the
processor – may make the difference in reducing the harm created by such breaches and in helping to comply with the GDPR.

Many of these lessons are mere common sense. Some of them require some time to implement, so the earlier the better, in the perspective of a potential application of the GDPR. Whether or not the GDPR is adopted, following the above lessons now should help companies best prepare themselves in the eventuality that the GDPR is adopted – either in its current version, or with amendments.

W. Gregory Voss is a professor of business law economics at Toulouse Business School, Toulouse University, and member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC), Toulouse, France.