The United States and the European Union have long had different philosophies on the collection and protection of personal data, which is defined broadly by the EU as any information relevant to an identified or reasonably identifiable natural person. The EU views individuals as having a fundamental right to the protection of their personal data. In the United States, the focus has always been on balancing the desire of individuals to have their personal data protected with the needs of businesses to use that data. The United States has also had a stronger commitment to the free speech rights of those who want to use or comment on lawfully acquired personal data.

The EU adopted a directive (an order for member states to adopt consistent legislation) on the protection of personal data in 1995, and U.S. companies with significant operations in the EU have struggled since then to find ways to accommodate the EU demands. The major problem has been, and continues to be, that the EU forbids the transfer of personal data about EU residents to countries— including the U.S.—that do not provide an EU-level of privacy protection. Even intracompany transfers are affected. The present options for U.S. companies include joining a Department of Commerce Safe Harbor program, under which companies must demonstrate an adequate privacy policy; conducting data transfers under EU-approved Standard Contractual Clauses, which many U.S. companies find too onerous; and adopting EU-approved, legally effective Binding Corporate Rules, which have also been unpopular in this country. While compliance under any of these methods has never been a pleasant exercise, most U.S. companies have found a way to cope.

The European Commission, the EU’s executive branch, has now proposed a new personal data regulation that will make life dramatically more difficult for an even greater number of U.S. companies. The regulation itself is lengthy and complex, with 91 articles preceded by 139 findings that explain the reasoning behind the regulation. While there may be some controversy over some of the proposals, this regulation has been under development for years and most observers expect it ultimately to be adopted without major changes. The remaining procedural hurdle of obtaining final approval by the EU’s Parliament and Council is expected to delay actual implementation for as little as 18 months or as long as four years, depending
on whom you ask. When finally adopted, the regulation, unlike a directive, will take effect throughout the EU without the need for country-by-country legislation. The regulation will make far-reaching changes that could impact any business collecting and using the personal data of EU residents.

This article provides a starting point for U.S. businesses that will need to find a way to deal with these changes. First, we discuss the broad scope of the EU Regulation and the risks and burdens it will impose on U.S. companies. Then we suggest some steps that U.S. businesses should be taking now to prepare for the change.

The Scope of Regulation

EU data privacy law has always applied to the activities of any company that has a place of business (or, in EU jargon, an “establishment”) physically located in the EU. However, under the existing directive, U.S. companies without an EU establishment are not subject to regulation when they collect the personal data of individuals who reside in the EU unless the U.S. company collects or processes the data using equipment located in the EU. As a practical matter, this excludes coverage for most small and mid-sized U.S. companies that collect personal data from EU residents only as a part of their normal online sales process.

The new regulation would expand coverage significantly. It distinguishes between data controllers and data processors: the controller is the person or entity in charge of the collection and use of data, while the processor is just that – the entity that actually performs the data operations. They can, of course, be the same or different entities. Under Article 3, the regulation will continue to cover “the processing of personal data by controllers or processors with an establishment in the EU.” Finding 19 states that an “establishment” in the EU involves “stable arrangements,” whether in the form of a branch or a separate corporate subsidiary.

The major change in scope is the extension of coverage to companies merely because they collect data from EU residents, even though they have no established operations in the EU. Under Article 3, the regulation will apply to the processing of personal data of residents of EU countries by a controller not established in the EU, where the processing activities are related to (a) the offering of goods or services to such EU residents; or (b) the monitoring of their behavior, which can include tracking and profiling internet activities for the purpose of analyzing or predicting preferences.

If an EU resident believes that a U.S. company has violated the regulation, she can choose (under Article 75) to bring suit in her home country, which is mandated to “enforce the final decisions” of its courts. While the enforceability of a judgment against a U.S. company presents thorny questions of international jurisdiction, this is not an empty threat. If the U.S. company had property in the EU, a European court could order the seizure of that property to satisfy the judgment. If not, the EU plaintiff would have to bring the judgment to an American court for enforcement against the company’s property here. A U.S. court could enforce the judgment so as long as the U.S. company did a non-trivial amount of business (had “minimum contacts,” in jurisdictional jargon) in the EU.
In addition to the risk of a lawsuit, a U.S. company that violated the regulation would be subject to significant administrative sanctions under Article 79. The sanctions are supposed to be painful – they are specifically required to be “effective, proportionate and dissuasive.” The penalties will vary depending on the nature of the violation, but can range up to one million euros or 2 percent of the violator’s worldwide turnover. As in the case of private judgments, the EU privacy authorities’ ability to collect such penalties would depend on the principles of international jurisdiction discussed in the previous paragraph.

Taken together, these changes present a clear danger for U.S. companies doing business in the EU. The coverage of the new regulation is broad, the penalties for noncompliance are severe, and the penalties may be enforceable against any U.S. company doing any meaningful amount of business with EU residents. Ignoring EU data privacy rules will no longer be a viable option.

The Regulatory Burden

At a high level, the regulation seeks to achieve objectives that enjoy widespread support: fair and transparent data collection, avoiding the collection of excessive amounts of data or the retention of data that is no longer needed, ensuring that collected data is accurate, requiring consent to the use of collected data, and ensuring that collected data is stored securely. While the U.S. shares those high-level objectives, U.S. law is also acutely aware of the commercial cost of pursuing those objectives and therefore seeks to strike a balance. There is no comparable sense of balance in the regulation. As a result, it lays down rules that protect individuals admirably but impose potentially significant new commercial costs and burdens on businesses. Some of the more significant changes are:

- **Consent.** Subject to some specific exceptions, personal data can be collected from an EU resident (referred to in the regulation as the “data subject”) only with affirmative consent. That basic notion is not new, but has now been expanded. Under Article 7, consent is no longer valid if there is a “significant imbalance” between the data controller and the data subject. While the scope of this equitable notion is not clear, Finding 34 expressly provides that it applies in any situation in which the data subject is “in a situation of dependence” on the controller, such as employment. The data subject also has the right to withdraw consent at any time. This right will impose on data collectors the significant burden of developing the technical ability to quickly locate and remove the data of any individual data subject who withdraws consent.

- **Notice and Response.** Under Article 14, a data controller that collects personal data has to provide the data subject with a detailed notice about the nature and purpose of the data collection. In some situations, this obligation can extend to notifying data subjects when a company acquires their personal data from a third party. Under Article 15, the data subject has the right to obtain from the data controller, upon request and without cost, a significant amount of information on the type of data being collected and retained and how it is being used. These requirements could impose a particularly difficult burden on any company that lacks uniform, documented, company-wide polices and procedures on its collection and use of personal data.

- **Rectification and Erasure.** Under Article 16, the data subject has the right to require that the data controller correct any personal data that is inaccurate, including the supplementation of any information that is incomplete. More significantly, under Article 17, a data subject has a relatively broad “right to be forgotten and to erasure.” If a
data subject properly exercises this right, the data controller must erase (or in certain cases store) the data subject’s personal data. If the controller has provided that information to a third party, or made it public, it has the obligation to take all reasonable steps to cause the data to be erased.

- **Limits on Direct Marketing.** Articles 19 and 20 attack head-on the increasingly popular commercial practice of using individualized information on consumers to develop targeted marketing strategies. Article 20 limits the right of companies to engage in automated processing of certain types of sensitive information (relating, for example, to location, economic situation, health, work or personal preferences) to create marketing profiles. Article 19 allows any data subject to object to the use of her personal data for direct marketing, even if none of the sensitive types of information are being used.

- **Data Security.** The regulation requires the data controller to adopt policies and procedures that ensure adequate data security and compliance with the administrative requirements of the regulation, and to provide prompt notice of security breaches. For the most part, these requirements track existing best practices under U.S. law. However, they do create the possibility of inconsistency regarding the exact data security requirements, since the EU Commission is entitled to establish the “state of the art” for data security by further regulation. In addition, they increase the administrative burden for data breaches by adding the requirement of reporting any breach to an EU supervisory authority, generally within one day.

- **Appointment of Representative.** Many third parties that do not have a place of business in the EU but collect personal data on EU residents will be required to appoint a “Representative” in the EU. There are exceptions to this requirement for controllers established in a country that provides EU-level privacy protection, controllers that employ less than 250 people, and controllers that “only occasionally” offer goods or services to EU residents (when, for example, the offering of goods or services in the EU is “ancillary” to the company’s main activities.) The appointment of a representative would be a more significant act than the typical appointment of an agent for service of process, since the representative must have the authority to deal with the EU data privacy authorities on behalf of the data controller.

- **Required Impact Assessment and Governmental Approval.** Under Article 33, “where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,” data controllers and processors will be required to perform a self-assessment of the impact of the proposed processing operations. Article 34 then provides that where the assessment indicates “a high degree of specific risk,” and under other limited circumstances, a data controller or processor must obtain prior authorization from the data supervisory authority of a member state before doing the processing. The supervisory authority has broad power to limit or even prohibit the processing. The scope of these somewhat vague requirements will be fleshed out by “standards and requirements” to be adopted by the EU Commission.

- **Continued Limits on Data Transfer to the U.S.** The regulation continues the existing limits on transferring personal data to any other country that the commission does not believe has adequate data protection laws. Since the U.S. will almost certainly continue to be on the list of disapproved countries, data collectors will continue to have to deal with the options discussed above if they need to transfer data to the U.S. The regulation may also eliminate the option of using individual employee consent to intercompany transfers.
Planning for the Change

Most observers think the final adoption of the regulation is two to four years in the future. However, the potential changes are so sweeping, and the potential costs of noncompliance are so severe, that it would not be prudent for any affected U.S. company to wait until the last minute to develop a plan for dealing with the regulation.

The high-level theme of the proposed regulation is one of limitation: In a technical environment that offers ever-expanding and increasingly sophisticated ways to collect and use personal data, the EU wants companies to abruptly head in the opposite direction, by limiting what personal data they collect and use and by developing the ability to respond to inquiries and requests from individual EU residents about the nature and use of their individual personal data. For many companies, this will require a fundamental change in the way that they collect, store and use personal data.

There are at least three specific steps that any affected U.S. company should be taking now to prepare for this change. First, each company should do a careful assessment of its internal data policies to ensure that it understands exactly what personal data it is collecting and how it is storing and using that data. In doing so, it must bear in mind that the regulation broadly applies to any information relating to an identified or reasonably identifiable natural person, whether it is in electronic form or written files. Second, each company should match its current data collection practices with its actual business needs, and develop and implement uniform, documented policies that ensure that it is collecting and retaining only personal data that is actually needed. Finally, each company should ensure that it is using generally accepted best practices, by U.S. standards, in the way that it provides data security. All of these steps have the dual advantage of improving the handling of data in the United States, while starting the process of preparing for the dramatic changes coming in the EU.