The GDPR – New EU Law on Personal Data

Wojciech Wandzel, Grzegorz Pobożniak, Paula M. Bagger

1. What is the GDPR?

The headlong push by European and American companies to collect and mine consumer data can be compared to the 19th century Alaskan gold rush. Exercising a different historical metaphor, Doug Fisher, an Intel executive, predicted that data would be to the 21st century what oil was to the 20th century, an engine for corporate growth, with one significant difference: "oil is definite while data is renewable." Databases are key corporate assets, particularly in technology companies, and an up-to-date, growing database can lead directly to an increase in sales. When the data being collected and processed is about individuals who may not be aware that personal information has been collected and is being used, serious privacy concerns accompany this growth.

In response to these concerns, the European Union (EU) has adopted sweeping new rules governing the processing of personal data concerning natural persons, which become effective on May 25, 2018. Regulation 2016/679, the General Data Protection Regulation or GDPR, was enacted to respond to a perceived need for privacy law change in the face of dynamic developments in personal data processing technologies. The GDPR will apply in all 27 member states of the EU. Its effects will be felt not only by EU companies but also non-EU companies who offer goods or services in the European market. U.S. companies need to understand the GDPR and the ways it will change how they handle personal data.

The GDPR is no less than revolutionary in the ways it protects personal data. Previously, personal data collection and processing in the EU was governed by EU Directive No 95/46/WE and enabling legislation passed by the member states. In general, it was far less restrictive in its regulation of the collection and processing of personal data. The obligations it imposed were less onerous and the sanctions for violation, imprecisely defined in the EU Directive, largely imposed by the member states.

The GDPR, by contrast, is an EU Regulation, not a Directive, and thus requires no implementation by the member states. Rather it applies directly in all EU member states. The basic rules governing the processing of personal data of natural persons will now be the same throughout the EU. National legislation will merely supplement the GDPR in order to conform procedural provisions to the administrative or judicial processes of member states or, in some instances, to allow for certain permissible exemptions, *e.g.,* special rules for small business compliance. Consequently, all of the EU (approximately 90% of the European market and over 20% of the global market) will be subject to the same substantive rules governing personal data processing.

Within the meaning of the GDPR, a "data controller" is the person or entity that "determines the purposes and means" of the processing of personal data; in most cases, it is the person or entity that collects the data from a client or customer. A "data processor" is the person or entity that "processes," *i.e.,* stores, digitizes, catalogs, etc., the personal data. A "data subject" is the individual whose personal data is at issue. United States companies that have a physical presence in EU member states, offer products or services to persons resident in the EU, or monitor the on-line activities of such persons will need to ensure that their operations comply with the GDPR.

2. Requirements.

There is insufficient space here to discuss, in detail, all the issues that will present themselves to U.S. companies coming into compliance with the GDPR; the number and types of issues will depend on the activities each company pursues. Particular attention must be paid, however, to those requirements that reflect a fundamentally new approach to personal data protection and thus may require significant changes in existing business practices. There are no detailed practical guidelines in the GDPR how to protect personal data, thus it is mainly entrepreneur's responsibility to evaluate what measures shall

be apply to preserve appropriate level of protection. The principal obligations that the GDPR imposes on companies subject to its requirements are:

(i) Ensuring that personal data is processed only where there is a "legal basis" to do so;
(ii) Incorporating the concepts of "privacy by design" and "privacy by default" in business operations and development efforts;
(iii) Safeguarding a newly created set of data subjects' rights;
(iv) Performing an impact assessment before commencing personal data processing that may where a given type of processing is likely to result in a high risk to the rights and freedoms of the data subjects;
(v) Designating a data protection officer, where required given the type of personal data being processed or scale of processing efforts;
(vi) Reporting personal data breaches to a supervisory authority within 72 hours of discovery.

Ensuring a "legal basis" for processing exists. The first obligation is basic and sweeps broadly: no personal data processing may occur in the absence of a "legal basis" for the activity. Consent of the data subject is perhaps the most important legal basis; others include processing necessary for the performance of a contract; processing necessary for compliance with a legal obligation to which the data controller is subject; or processing necessary to protect the vital interests of the data subject. Processing personal data without such a lawful basis is unlawful and will subject both processor and controller to the GDPR's most severe sanctions.

Implementing "privacy by design" and "privacy by default." "Privacy by design" and "privacy by default" are concepts are being incorporated into European privacy law for the first time. Briefly speaking, "privacy by design" means that an enterprise must, at the planning stage of new business operations or the implementation of new products or applications, assess the impact of the planned action on personal data protection and take adequate steps to ensure the security of the data. The goal is for personal data protection to be built into each product or service offered to a person who resides in the EU. "Privacy by default" means that each product or service offered in the EU must have default privacy settings, designed to offer maximum user protection. With a compliant product or service, the user will not need to choose greater protection of personal data—because the default level is maximum protection; rather, the user will be allowed to elect a lower level of personal data protection.

Safeguarding data subject rights. The GDPR imposes new obligations on companies to honor newly created substantive rights afforded data subjects. These new rights include the right to extensive disclosure in connection with a request to process personal data (Arts. 13 and 14 of the GDPR), a right to access one personal data, a right to rectification of incorrect personal data, a right to move personal data to a new controller, a right to restrict processing, and a right to the deletion of personal data. The right to deletion may be the most difficult to be implement, particularly in view of the regular, automated creation of back-up files of operating systems. (Indeed, many IT professionals argue that effective compliance with the obligation to delete is simply not possible). It should be expected that supervisory authorities will publish interpretations and guidelines in the future about this and other obligations.

Performing impact assessments. Where a type of processing (in particular one using new technologies or altering the nature, scope, context or purposes of the processing) is likely to result in a high risk to the rights and freedoms of natural persons, the GDPR requires the data controller, prior to the processing, to carry out an assessment of the impact of the contemplated processing operations on the protection of personal data. In accordance with the GDPR's accountability principle, the enterprise will have to be able to demonstrate, in the course of an inspection, that the it performed such an assessment and took relevant steps to ensure the security of the personal data. Should this assessment indicate that the contemplated activity would result in a high risk to the rights and freedoms of natural persons in the absence of measures taken to mitigate the risk, the data controller will be required to consult the supervisory authority prior to processing. The authority will issue relevant recommendations which the controller will have to comply with. Failure to perform an impact assessment is a major

breach of the GDPR and puts the controller at the risk of severe sanctions which the supervisory authority may impose.

Designating a data protection officer. Where the core activities of the data controller or processor require the regular and systematic monitoring of data subjects on a large scale or consist of processing especially sensitive categories of data (information about racial or ethnic origin, political opinions, criminal records), the GDPR requires the appointment of a data protection officer in each member state in which the enterprises does not reside but data subjects do. The data protection officer provides a point of contact between the US enterprise, the data subjects, and the supervisory authorities in the member state and is responsible for ensuring that personal data is processed in accordance with the GDPR as applied in that member state.

Reporting data breaches. The last major new requirement introduced by the GDPR is the obligation to notify supervisory authorities of personal data breaches. In the event personal data protection is breached, the data controller must report it to the supervisory authority within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to the rights and freedoms of natural persons, the controller must also communicate the breach to the data subjects without undue delay. A failure to provide required notification of a personal data breach itself constitutes a separate violation of the GDPR, which may itself result in sanctions, whether or not any sanctions are imposed for the personal data breach.

3. Penalties and other sanctions

Previous EU regulations left the imposition of sanctions for personal data processing breaches to member-state law. The GDPR introduces uniform penalties and other sanctions applicable throughout the EU. Very significant administrative fines, to be imposed by the regulatory authorities of member states, will be imposed not only on EU companies, but also non-EU (including U.S.) companies.

The administrative fines authorized by the GDPR can be as high as 2% of the total worldwide annual gross revenue in the event of a breach of a failure to (i) obtain consent for processing personal data of a child below the age of 16, (ii) comply with the privacy by design and privacy by default rules as required by the GDPR, (iii) use services of a contractor which certifies that its personal data processing complies with the GDPR, (iv) maintain a record of processing activities, (v) cooperate with the supervisory authority, (vi) implement measures to ensure data security, (vii) report a personal data breach to the supervisory authority, (viii) notify a data subject of a personal data breach, or (ix) assess the impact of a personal data breach.

Violations of the GDPR's basic principles for data processing and violations of the rights of data subjects, including the right of access to one's personal data, the right to rectification and deletion of personal data, the right to demand restriction of processing, and the right to data portability) are subject to administrative fines up to 4% of total worldwide annual gross revenue.

In addition to this scheme of administrative fines, the GDPR also authorizes civil claims by natural persons who allege that their personal data was processed in violation of the GDPR's requirements. Money damages will be awarded for both economic loss and emotional distress and other intangible loss found to have been caused by a violation of the GDPR. The availability of a private right of action under the GDPR will open businesses, including U.S. businesses processing the personal data of EU residents, to litigation in European courts. In particular, one may expect a large number of court cases for the remedying of intangible losses, which in the civil law systems prevalent in the EU are more easily established than losses to tangible property.

Summary

The GDPR imposes a number of new and unfamiliar data privacy obligations on companies operating in the European Union and metes out very harsh sanctions for violations. At present, it is difficult to foresee to how effectively the new regulations will be implemented as well as how they will be applied in practice. The GDPR is controversial in the EU and has been greeted with skepticism by many EU

enterprises, which question the extent to which the new approach to data privacy will actually improve personal data protection and how the results achieved will measure up against the substantial burdens imposed. Nevertheless, every company in the EU is working hard to adapt its operations to the new regulation so that it will be in compliance by May 25, 2018, and U.S. companies will do well to follow suit.

This article originally appeared on:
https://www.americanbar.org/groups/litigation/committees/commercial-business/articles/2018/gdpr-new-eu-law-on-personal-data.html