INTERNATIONAL LAW NEWS
WWW.AMERICANBAR.ORG/INTLAW

EU's General Data Protection Regulation (GDPR): Key Provisions and Best Practices

Vol. 46 No. 2

By Aaron Schildhaus

Aaron Schildhaus Counsel at Scharf Banks Marmor LLC. He serves on the Council of the American Bar Association's Section of International Law and is the liaison from the Section to the Council of Bars and Law Societies of Europe (CCBE). He served as Chair of the Section of International Law in 2008–2009.

Whether or not your company is doing business in the European Union (EU), it will be affected by the EU's General Data Protection Regulation (GDPR). Why? Because the scope and reach of the regulation are global and likely to touch companies everywhere.

On May 25, 2018, the GDPR comes into full force and effect, and companies around the world are preparing for it. Failure to comply with this new law will put companies at risk for enormous fines and penalties: up to the greater of 4 percent of annual global revenues or EUR 20 million for data controllers and up to the greater of 2 percent of annual global revenues or EUR 10 million for data processors.

This article reviews some of the following areas covered by the GDPR: its extraterritorial effect, the lawfulness of data processing, dealing with a personal data breach, data rectification, data portability, the right to be forgotten, data protection by design, and data protection impact assessments. Because a discussion of these provisions only scratches the surface of this far-reaching regulation, it is suggested that incorporating relevant GDPR requirements into the operating procedures of companies worldwide should be considered as best practices in the field of cybersecurity, data protection, and privacy. Practitioners also should keep in mind that the regulation is very comprehensive and many of its provisions overlap and interconnect. Therefore, a careful study and understanding of the regulation in its entirety is recommended.

Background

The GDPR replaces the existing Data Protection Directive 95/46/EC (Directive), which has been the standard for data protection and data privacy in the EU since it came into force in December 1995. U.S. companies now in compliance with the Directive, including the more than 2,400 companies that have qualified for the EU-U.S. Data Privacy Shield and its analogue, the Switzerland-U.S. Privacy Shield, should be aware that compliance with the current data protection regime will not be sufficient, in and of itself, to qualify under the GDPR.

The GDPR was designed to deal with the growing need to further protect Europeans from being compromised by the misuse of personal data in the possession of organizations. It is harmonizing privacy and data security laws across Europe and reshaping the way entities across the region approach data protection. The intent of the GDPR is set out in Article 1, which "lays down rules" relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data . . . (and it) . . . protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Because the GDPR is a regulation, and not a directive, it is directly applicable in all EU Member States. The GDPR applies extraterritorially by its terms.

Indeed, it is noteworthy that the United Kingdom's upgrading of its Data Protection Act with its Data Protection Bill essentially conforms to the GDPR so that its businesses can remain competitive with others in the EU despite Brexit. In any event, the U.K.'s exit from the EU will not take place before the GDPR takes effect in May; therefore, U.K. businesses will be subject to the GDPR as of May 25, too.

Extraterritoriality

The GDPR's implementation will have a profound effect on data protection and privacy not only in Europe but also worldwide, given the transborder realities of electronic data management and processing and the regulation's new extraterritorial provisions. The GDPR applies to all companies, regardless of location, that process the personal data of data subjects residing in the EU. Article 3 states that the GDPR also applies to the processing of personal data of data subjects in the EU by controllers and processors in the EU, wherever the processing takes place, whether or not in the EU.

Another extraterritorial provision of the GDPR is that the regulation applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to the offering of goods or services to EU citizens (whether or not payment is required) and the monitoring of behavior that takes place within the EU. Previously, under the Directive, territorial applicability was ambiguous, referring to data processing in the context of an establishment. The extraterritoriality of the regulation is now clear; moreover, non-EU businesses processing the data of EU citizens will have to appoint a representative in the EU, as given in Article 27.

The GDPR and related EU and country legislation and regulations contain a myriad of requirements and provisions, all of which merit close examination by companies that have direct or indirect operations in Europe. Many global companies already recognize that it makes sense to incorporate practices and policies that will help protect themselves against claims of violating statutory standards of conduct and ethical norms by governmental entities or individuals. The potentially crippling fines that noncompliant companies would expose themselves to are reason enough for their boards of directors to mandate compliance with the GDPR.

Lawfulness of Processing

For the processing of data to be legal, Article 6 requires at least one of the following conditions:

- Consent – the data subject has given consent to the processing of the data;
- Contract – the processing is necessary for the performance of a contract to which the data subject is a party or into which the data subject is seeking to enter;
- Legal Obligation of Controller – the processing is necessary for compliance with a legal obligation of the controller;
- Protection of Vital Interests – the processing is necessary to protect the vital interests of the data subject or of another natural person;
- Public Interest – the processing is necessary for the performance of a task carried out in the public interest; or
- Legitimate interests of controller or third party – subject to the data subject's fundamental rights and freedoms requiring protection, particularly those of a child.

Relative to the foregoing, a number of requirements are imposed on the controller. Among those, Article 12 requires any request for the data subject's consent to be given in a concise, transparent, intelligible, and easily accessible form. Further, the consent must be given for one or more specific purpose under Article 9(2), and the forms providing for data subject consent must be clear and intelligible under Article 12(7).

It should be noted that Article 15 provides data subjects the right to obtain a free report regarding the type and purpose of data, as well as the names of the data processors. Moreover, Article 7(3) requires the process for withdrawing consent to be as easy granting it.

Personal Data Breach

Cybersecurity best practices include not only minimization of cyber risks but also comprehensive and detailed plans regarding how best to handle a breach if one occurs. A personal data breach is defined in Article 4(12) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Article 33 sets forth the notice of breach obligations of data processors with respect to their Supervisory Authority, which are the relevant independent public authority or authorities responsible for monitoring the application of the GDPR in a given country. Articles 51–68 provide a comprehensive description of supervisory authorities. Article 68 describes the EU Data Protection Board. Articles 33 and 34 set forth the obligations with respect to data subjects and to their data controllers.

It is recognized that not all data breaches harm the data subject; however, in the event of a personal data breach that could result in a risk to the rights and freedoms of a data subject, the data processor is required under Article 33 to notify the Supervisory Authority "without undue delay" and no later than 72 hours from learning of the breach. If it fails to do so in this time frame, it must accompany the notice with the reasons for the delay.

The data processor also must notify the data controller "without undue delay" and must notify the data subject, also without undue delay and in clear and plain language, of the nature of the breach. Notice to the Supervisory Authority and to the data subject must identify the data protection officer or other contact where more information can be obtained, must describe the likely consequences of the data breach and must described the measures, including, where appropriate, those to mitigate damages, that the data controller has taken, or intends to take, as a result of the breach.

The data processor must provide to the Supervisory Authority documentation regarding any personal data breaches, their effects, and the remedial actions it has taken so that the authority can verify the extent to which the processor is complying with its GDPR requirements.

The Right to Rectification

Article 16 provides that the data subject shall have the right to obtain from the controller "without undue delay" the rectification of inaccurate personal data. The data subject also has the right to have incomplete personal data completed, which includes providing a supplementary statement.

The Right to Erasure (Right to Be Forgotten)

Among the many rights of the data subject vis-à-vis the controller is the right to be forgotten. Article 17 provides that the controller must erase personal data without undue delay where the personal data is no longer necessary for the purposes collected or where the data subject withdraws consent and when there is no other legal ground for the processing. If the data subject exercises the right to object pursuant to Article 21 dealing with profiling and direct marketing, or if the personal data has been unlawfully processed, the data subject may invoke the right to erasure. The right to erasure applies as well if the personal data must be erased to comply with an EU or Member State law to which the controller is subject or where the personal data was collected relative to a child under the age of 16 as set forth in Article 8(1).

The right to erasure does not apply to the extent that processing is necessary to exercise the right of freedom of expression and information or to comply with a legal obligation that requires processing by EU or Member State law to which the controller is subject. Exemptions under Article 17(3) clarify that it does not apply to the performance of a task carried out in the public interest or in the exercise of official authority or for reasons of public interest in the area of public health. It also exempts archival purposes in the public interest, for scientific or historical research, for statistical purposes, or for the establishment, exercise, or defense of legal claims.

Data Portability

Provided that it does not adversely affect the rights and freedoms of others and that it does not consist of processing necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, the data subject has the right under Article 20 to receive all personal data he/she has provided to a controller, in a structured, commonly used, and machine-readable format, and has the right to transmit such data to another controller where the data processing is carried out by automatic means. Such transfers must be based on one or more of the following:

- consent received from the data subject to process his or her personal data for one or more specific purposes pursuant to Article 6(1)(a);
- explicit consent received from the data subject, pursuant to Article 9(1)(1), to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or data concerning a natural person's sex life or sexual orientation; or
- processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, as consistent with Articles 6(1)(b) and 20(1).

Where technically feasible, the data subject has the right under Article 20(2) to have the personal data transmitted directly from one controller to another. This right of data portability is without prejudice to the right set forth in Article 17 regarding the right to be forgotten.

Data Protection by Design and by Default

Data protection by design under the GDPR means that data protection must be a consideration from the onset of the designing of systems, rather than an addition. The controller is required, under Article 25, to implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimization in an effective manner, and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.

The controller must implement measures to ensure that only the data necessary for the specific purpose of the processing are processed. As specified in Article 25(2), this includes the amount of data collected, the extent of its processing, and the data's storage period and accessibility.

Data Protection Impact Assessments and Prior Consultations

Article 35 requires the controller to take into account the nature, scope, context, and purposes of any proposed processing. If it is likely to result in a high risk to the rights and freedoms of natural persons, the controller must carry out an assessment of the proposed processing on the protection of personal data and must seek the advice of the data protection officer. These Data Protection Impact Assessments (DPIAs) are absolutely required under Article 35(4) for specific processing operations that are publicly listed by the Supervisory Authority. Likewise, Article 35(5) provides that the Supervisory Authority may establish a public list of the kind of processing operations for which no DPIA is required.

The DPIA must contain:

- a systematic description of the proposed processing operation and its purposes, including the legitimate interest of the controller;
- an assessment of necessity and proportionality of the processing operations relative to the purposes;
- an assessment of the risks to the rights and freedoms of the data subjects; and
- the measures proposed to address the risks, including safeguards, security measures, and mechanisms to ensure personal data protection and compliance with the GDPR.

Article 36 reiterates the requirement for the controller to consult with the Supervisory Authority prior to processing where a DPIA indicates that the processing would result in high risk if no mitigating measures are taken by the controller. If the Supervisory Authority believes that the intended

processing would infringe the regulation, particularly where the controller has insufficiently identified or mitigated the risk, the Supervisory Authority has up to eight weeks from the controller's request for consultation to provide written advice to the controller and the processor and may extend the period until it has obtained the requested information. The Supervisory Authority may exercise any of its Article 58 powers in this process.

Data Protection Officer

Depending on the nature, scope, purposes, and core activities involved, controllers or processors may be required to appoint a data protection officers, whose qualifications and responsibilities are set forth in Articles 37–39.

Under the GDPR, it will not be necessary, as is currently the case, for data processors to submit notifications and registrations to each local Data Processing Authority (DPA) of data processing activities, nor will it be a requirement to notify or obtain approval for transfers based on Standard Contractual Clauses (SCCs).

Instead, there will be internal record keeping requirements. Also, the appointment of a Data Protection Officer (DPO) will be obligatory only for those controllers and processors whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale or special categories of data or data relating to criminal convictions and offenses. The DPO must be appointed based on professional qualities, particularly expert knowledge on data protection law and practices, and may be a staff member or an external service provider. The DPO's contact details must be provided to the relevant DPA. In addition, the DPO must be provided with appropriate resources to carry out its tasks and maintain his/her expert knowledge. The DPO must report directly to the highest level of management and must not carry out any other tasks that could result in a conflict of interest.

The GDPR is changing the international legal landscape and is affecting businesses, governments, organizations, and individuals in many ways, and its impact will only increase. The issue of data protection and privacy will continue to be a core concern of persons and entities worldwide. Constant and in-depth review and incorporation of the GDPR's approach as best practices will help organizations as this critical area continues its rapid evolution.

***

Aaron Schildhaus is Counsel to Scharf Banks Marmor LLC, a Chicago law firm specializing in corporate litigation and transactions. His practice is focused on US – EU data protection and privacy compliance, FCPA compliance and due diligence, and international transactions involving the US, Europe, Africa, India, the Middle East and Latin America, representing NGO's and large and small corporations in the US and abroad. He is past Chair of the ABA Section of International Law and has spoken frequently internationally, and written numerous articles, on data protection in Europe and on a wide variety of other business related legal topics.