8-in-8 Recent Trends in European Law and Policy Alert Series The EU's Data Protection Regulatory Big Bang: The GDPR Comes Into Force

MAY 23, 2018

This is the inaugural issue of WilmerHale's 8-in-8 Recent Trends in European Law and Policy Alert Series. Over the next eight weeks, our attorneys will share insights on current and emerging issues affecting companies doing business in Europe and across the Atlantic. Attorneys from across various practice groups at the firm will offer their take on issues ranging from Brexit to Big Data to EU energy market regulation. WilmerHale has offices in key European capitals, including Brussels, Berlin, Frankfurt and London, as well as lawyers qualified in a range of European countries. With one of the leading European law and policy practices in the world, we follow and work on a broad range of EU legal and policy issues, including data protection and privacy, competition, trade, technology, intellectual property, financial services, and a range of other EU and transatlantic regulatory and policy challenges that our clients face.

The European Union (EU) General Data Protection Regulation (GDPR, available here) will take effect Friday, May 25. The new Regulation will impose a strict and far-reaching data protection regime with extraterritorial effect. Compliance is mandatory, with fines for non-compliance as high as €10 million or 2% of worldwide consolidated group turnover, whichever is the highest, or €20 million or 4% of worldwide consolidated group turnover, again whichever is the highest.
Below, we discuss some of the background to the Regulation and its relevance to companies in all sectors that do business in or with Europe.

Before the Regulation, there was a Directive. The GDPR builds on the existing data protection framework established by the EU's Data Protection Directive in 1995 (available here). Pursuant to that Directive, the Member States of the EU enacted laws prohibiting the processing of personal data (i.e., any data related to a physical person and permitting the latter's identification, directly or indirectly) unless this processing could be justified based on the listed and limited grounds in the Directive. As long as the Member States respected the basic principles laid down in the Directive, they were free to introduce rules specific to their own jurisdiction. In addition, the broad principles of the Directive were sometimes given divergent interpretations by the data protection authorities of different Member States. As a result, companies have been facing a patchwork of rules impeding

the free flow of personal data within the EU, which the Directive had been meant to safeguard.

Data protection elevated to the rank of fundamental human right. The EU adopted the Charter of Fundamental Rights in 2000 (available here). It became legally binding in December 2009. The Charter lists the fundamental rights of everyone living in the EU and includes some rights that were not formally recognized before. Among these, Article 8 of the Charter provides for a right to personal data protection, separate from the fundamental right to privacy, which is enshrined in Article 7 of the Charter.

The Regulation brings about a more restrictive framework. In light of the Charter's elevation of data protection to a fundamental right, the GDPR's main focus is to ensure the strong protection for personal data across the EU with one Regulation. As a result, the GDPR retains all the basic protective principles laid down in the Directive, while providing for new rights and considerably strengthening the enforcement of these principles and rights.

New rights for individuals – new obligations for companies. The GDPR provides for new rights, such as the right to data portability, meant to ensure that individuals can freely transfer their data to new service providers. Companies will have to address these new rights, as well as the new obligations to conduct data protection impact assessments and to appoint independent data protection officers where required, and to report data security breaches to authorities and inform individuals about them, where required. More fundamentally, the GDPR changes the current balance of responsibilities between authorities and companies. Under the current system, companies in most Member States had to inform the authorities about their processing and to respond to (rare) follow-up questions by the authorities. The GDPR makes companies responsible for self-assessment of their processing of personal data, with the risk of liability and substantial fines if they get it wrong.

Increased sanctions. It is generally accepted that while a number of companies made considerable investments to respect the Directive's data protection principles, some only paid lip service to the rules. The GDPR aims to put an end to that by conferring upon national data protection authorities the power to impose extremely high fines, modeled on EU antitrust fines. Depending on the infringement, these fines can be as high as €10 million or 2% of worldwide consolidated group turnover, whichever is the highest, or €20 million or 4% of worldwide consolidated group turnover, again whichever is the highest. A number of data protection authorities have already announced their intention to use their new fining powers as soon as possible after May 25. Based on past experience with competition law enforcement, once one authority imposes high fines, it can be expected that others will want to follow, for fear of appearing to be less serious enforcers.

Is existing guidance satisfactory? In the months before the entry into force of GDPR, the Article 29 Working Party has adopted (or has been in the process of adopting) a number of guidelines (available here) to provide guidance to companies on various topics:

- Data Protection Impact Assessment
- Data Portability
- Data Protection Officers

- Lead Supervisory Authority
- Application and Setting of Administrative Fines
- Breach Notification
- Automated Individual Decision-making and Profiling
- Transparency
- Consent
- Transfers
- Accreditation of Certification Bodies

These guidelines offer valuable insight into the thinking of the enforcers and are required reading for data protection professionals. Most of them, however, are formulated in fairly theoretical and vague terms, and lack real-life examples. Although they are not legally binding, companies disagreeing with some of the interpretations provided in these texts can expect an uphill battle.

A more coherent framework? The GDPR should bring about greater harmonization of data protection law across the EU than the Directive did, since the rules contained in the Regulation are directly applicable and enforceable in Member State courts, as from May 25, in all EU Member States – there is no legal requirement for domestic implementation of the GDPR's rules. However, the GDPR still leaves room for Member States to maneuver to adopt additional regulation on specific topics (such as the age limit under which children are afforded added protection). In addition, the GDPR is too generic to put a complete end to existing divergences of interpretation among data protection authorities. The GDPR puts a number of procedures into place to try and achieve more consistent application and enforcement of the rules. It remains to be seen how these procedures will work in practice. Unfortunately, at this stage and based on the work done to date on the guidelines noted above, it looks like efforts toward consistency risk being achieved at the expense of flexibility and reasonable interpretations that have prevailed in some Member States under the Directive.

Are the enforcers ready? Currently, only a minority of Member States have adopted national laws to adapt their existing framework to the GDPR. However, many more are expected to modify their laws in the coming weeks. For the remaining countries that are months, if not years, away from enacting new rules, careful analysis is required, for example to determine whether the data protection authorities concerned would be able to impose the GDPR's new fines without any change in existing national law. The European Commission has announced that it will move swiftly to require lagging Member States to adapt their domestic laws and procedures to the requirements of the GDPR. In the meantime, companies should be able to rely on compliance with the GDPR to defend their data protection practices and procedures even in Member States that have not yet adapted their own enforcement practices.

Do enforcers have the means to enforce the GDPR? In many countries of the EU, the entry into force of the GDPR will not be accompanied by an increase in the local data protection authority's resources and manpower, raising questions as to its ability to effectively enforce the rules. However, some authorities, like the Irish Data Protection Commissioner and the UK's ICO, have obtained additional resources, while other authorities, like the French CNIL, already have significant staff. In

addition, authorities will no longer have to review notifications of processing or data transfer activities by companies and may therefore be able to re-direct existing resources to investigations and enforcement. Nevertheless, the high number of expected breach reports the authorities are likely to receive starting May 25 will present an initial challenge to effective enforcement.

Will there be a grace period? Many companies have been working hard to comply with the GDPR. Given the amount of work involved, there have been calls for a grace period after May 25. These calls are unlikely to receive a formal positive answer from enforcers. Their official point of view is that the GDPR was adopted more than two years ago and companies have had ample time to adapt, bearing in mind that many of the GDPR's principles were already contained in substance in the Directive (see the European Data Protection Supervisor's statement, available here). However, the French CNIL has announced that it will not, in the first months, sanction companies for breaches of the new rights and obligations introduced by the GDPR (such as the right to portability and the obligation to conduct data protection impact assessments – press report available here).

Should companies fear the GDPR's entry into force? GDPR enforcement will likely be gradual. Preeminent new (digital) economy multinationals with access to the data of hundreds of millions of persons will likely be in the enforcers' sights from the start. But it can be expected that domestic financial institutions and utilities (e.g., banking, insurance, energy and telecommunications and media companies) will not be far behind as enforcement targets. This is especially true for authorities wanting to make their mark quickly. New cooperation mechanisms are required by the GDPR for enforcement against large multinationals that process the personal data of citizens across the EU, which are likely to prolong such enforcement procedures. This is not to say, however, that other companies have nothing to fear. Customer or employee complaints or security breach reports may cause any company that processes personal data of EU residents to jump to the head of the enforcement queue.

Regulatory developments beyond GDPR. The GDPR is not the last word on IT security and privacy-related obligations for many companies. Other developments worth following include the current discussions on the ePrivacy Regulation (the EU Council released its draft version of the proposal on May 11, 2018, available here), the successor of the ePrivacy Directive (aka "the cookie Directive," available here). Also worth attention is the EU Commission's initiative to promote collective redress procedures (as a European alternative to US-style opt-out class actions), which is now set to include damages claims for the violation of the GDPR (the EU Commission's proposal is available here). Finally, information professionals will also want to follow the discussions on the "EU Cybersecurity Act," the proposal for a Regulation strengthening the mandate for the EU Agency for Cybersecurity ENISA and setting up the a European Cybersecurity Certification Framework (the Commission proposal can be found here.).

In summary, May 25 will mark a milestone in the more onerous and all-encompassing application of EU data protection rules to companies. It carries both the risk of an inflexible, overbroad regime that applies the same high compliance requirements to all, and the seriousness of purpose that new fining powers will give to enforcement of the individual right to personal data protection in the EU, with the possibility of even more detailed data protection and data security requirements to

come.

Authors

Frédéric Louis

PARTNER

frederic.louis@wilmerhale.com

+32 2 285 49 53

Christian Duvernoy

RETIRED PARTNER

christian.duvernoy@wilmerhale.com

+32 2 285 49 06

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207

Itsiq Benizri

COUNSEL

itsiq.benizri@wilmerhale.com

+32 2 285 49 87