THE NATIONAL
LAW JOURNAL

JUNE 20, 2018

Online Feature

An ALM Publication

National Variations Further Fragment GDPR

As long as the legal landscape is unfolding, supervisory authorities will hold off from the kinds of "true" enforcement action possible only under settled legal frameworks.

BY JAN DHONT AND LAUREN CUYVERS

The EU General Data Protection Regulation was portrayed as providing regulatory uniformity: The new legal regime would consist of a single set of rules together with enforcement through a "one-stop-shop" mechanism, enhancing legal certainty. The reality, however, appears to be different, and there may be less consistency and regulatory coherence than hoped.

The GDPR still leaves the member states a great degree of legislative freedom by allowing and even requiring national implementing legislation in a number of situations. For instance, member states are free to introduce specific conditions or limitations for the processing of biometric, genetic or health data; to create their own protection regimes for employee data and research and/or statistical data; and to pass local restrictions to the rights the GDPR grants to individuals. In addition, member states are required to establish supervisory authorities and to provide them with the resources required to effectively exercise their investigative and sanctioning powers. Businesses that are active in the EU market will not only have to comply with the GDPR but also with national privacy legislation in the countries where they operate.

By May 25, only a third of EU member states had met the deadline and passed GDPR implementing legislation—half of those mere days before. Front-runners were Germany, Austria, Slovakia and Belgium. The U.K. initiated its drafting process well in advance in mid-2017, but found itself subject to delays causing its effectively finalized data protection bill to receive "royal assent" (i.e., the last formality required for full passage) only on May 23. Sweden, Poland, the Netherlands, Denmark and Croatia passed GDPR implementation statutes in May. The remaining member states still find themselves in draft stage, with a few countries (including France and Italy) close to adoption. In most of the remaining member states (with isolated exceptions such as Bulgaria), draft GDPR legislation is in an advanced stage.

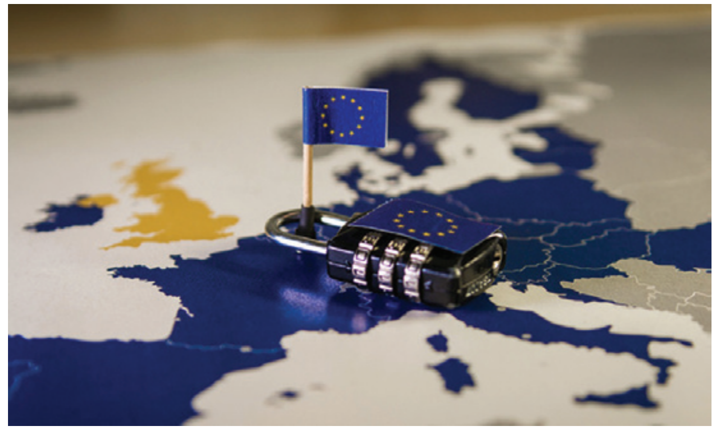

JAN DHONT


LAUREN CUYVERS

Additionally, the GDPR will apply not only in the European Union, but throughout the entire European Economic Area, which includes the EU member states and three European Free Trade Association member states (Iceland, Liechtenstein and Norway). In order for the GDPR to formally apply in the EFTA countries, and for the EFTA members to implement national GDPR legislation, the GDPR must be incorporated into the EEA Agreement. Despite efforts to incorporate the GDPR into the EEA Agreement before May 25, the process is still ongoing and is not expected to be completed before July 1.

Key highlights in national implementing legislation include GDPR deviations and specifications in individual rights restrictions and automated decision-making, biometric, genetic and health data, employee and/or HR data, class actions, administrative fining procedures and child's consent. Some examples include:

- Several member states lift the prohibition to process health data without the individual's prior consent when such data is necessary for medical treatment or diagnosis, or to ensure high-quality standards for the health care industry and medicinal products.
- The Dutch GDPR implementing act lifts the prohibition to process biometric data (which is considered sensitive data used to uniquely identify a person) without prior consent when such data is needed for authentication or security purposes. This could, for instance, cover access control mechanisms to a company's premises.
- Several member states have provided that sensitive employee data can be processed without prior consent when needed in the context of workers' reintegration or assistance in case of disability or illness, or to comply with social security, taxation and other legal requirements where the individual has no overriding interest in not processing such data.
- The requirement to appoint a data protection officer was further tailored in Germany, where the appointment of a DPO was already largely required before the GDPR. Germany's GDPR act provides that companies that employ at least 10 persons who process data, perform processing that requires a Data Protection Impact Assessment, or (anonymously) transfer or process data for market or opinion research must appoint a DPO.
- Most member states have lowered the minimum age at which children can provide legally valid consent for information society services to the minimum age permitted by the GDPR, 13 years old.
- From a procedural perspective, several GDPR implementing laws allow for "class actions" through which individuals mandate a nonprofit organization (e.g., a consumer rights organization) to represent them in regulatory and/or legal proceedings on their behalf. Member state implementing legislation also occasionally provides procedural rules for regulatory proceedings before the national Supervisory Authority, including appeal options, and certain specifics for administrative fines.
- Both the Austrian and Hungarian statutes indicate that their local supervisory authorities should issue warnings before resorting to fining (or other corrective) powers, especially for first-time violations. While the enforceability of these limitations on Supervisory Authorities' powers may be questionable as a matter of EU law, it currently forms an express part of Austrian and Hungarian GDPR statutes.



Businesses whose operations primarily focus on eastern and southern European markets will have to be patient before obtaining certainty on applicable national legal frameworks. The expectation, however, is that as long as the legal landscape is unfolding—and even in regions where GDPR statutes have been finalized—supervisory authorities will hold off from the kinds of "true" enforcement action possible only under settled legal frameworks, barring of course action undertaken in response to perceived serious misconduct.

Nevertheless, businesses should remain diligent and be aware that as of May 25, there is no longer a legal impediment for authorities to take action on the GDPR and/or implementing legislation where it exists, and companies should continue to work toward a compliance strategy.

Jan Dhont, *a partner in Alston & Bird's Brussels office, works with public and private companies in the EU and worldwide to resolve legal issues.* ***Lauren Cuyvers*** *is an associate in the Brussels office and a member of the privacy and data security group.*