COVINGTON

THE NEW EU DATA PROTECTION LAW: 10 THINGS YOU NEED TO KNOW

The General Data Protection Regulation (GDPR) was 5 years in the making. It has 91 Articles that run to 204 pages. Here are 10 things you need to know:

1. Agreement reached.

On December 15, 2015, the EU institutions agreed to the text of the GDPR. The GDPR will apply directly in all Member States two years after entry into force, which is expected in the coming months.

2. Global reach.

In addition to processing in the context of an EU controller or processor, the GDPR will apply to processing activities by non-EU controllers and processors that relate to the offering of goods or services to individuals in the EU or the monitoring of their behavior.

3. Stiff penalties.

Maximum fines for violating the GDPR will be 4 percent of an undertaking's total worldwide turnover or 20 million EUR—whichever is higher.

4. Oversight.

Instead of the hoped-for "one-stop-shop," which would have allowed organizations to interact with only one data protection authority (DPA), oversight under the GDPR will involve one "lead" and possibly several "concerned" DPAs and a complicated cooperation mechanism.

5. More rights for individuals and scope for class actions.

Individuals will have more rights under the GDPR, including a right to data portability, a "right to be forgotten," and a right to restrict processing. Group claims will be possible, subject to Member State law, and the right to lodge a complaint and the legal remedies will be strengthened.

6. International transfers.

The core restriction on transferring personal data to "non-adequate" countries outside the EU remains in place. The new law also expressly restricts transfers in response to non-EU judicial and administrative procedures. There are some improvements, including: Binding Corporate Rules (BCRs) are now expressly recognized as a data transfer mechanism; certain formalities in relation to using BCRs and model clauses have been dropped; and there is a new derogation for transfers based on "legitimate business interests."

7. Stricter substantive rules.

Rules about obtaining consent are more detailed. Organizations will have to work harder to demonstrate that personal data is processed on the basis of their "legitimate interests." The purpose limitation principle continues to apply, and profiling will be restricted and subject to specific rules.

8. Increased accountability, including a duty to notify of data breaches.

Controllers will be required to "demonstrate compliance." Existing registration requirements will be replaced by more elaborate internal record-keeping obligations. Some organizations must appoint data protection officers. Certain processing will require organizations to conduct a data protection impact assessment. Controllers will need to comply with "privacy by design" and "privacy by default" requirements. And there is a new mandatory breach notification obligation and greater emphasis generally on ensuring transparency.

9. Direct obligations on processors.

Processors now have direct, statutory obligations (not just contractual). Processors and controllers are jointly liable for damages caused by their processing activities.

10. One law, but with some differences.

Because it is a regulation, the GDPR will have direct effect in all EU Member States. However, Member States are allowed to adopt national rules in some important areas, including on procuring consent from minors, the handling of HR and health data, and the treatment of scientific research.

If you have any questions concerning the GDPR, please contact the following members of our Data Privacy and Cybersecurity practice group:

Jetty Tielemans	+32 2 549 5252	htielemans@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Monika Kuschewsky	+32 2 549 5249	mkuschewsky@cov.com
Kristof Van Quathem	+32 2 549 5236	kvanquathem@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com