COVINGTON

The New EU Data Protection Law: Key Elements for Business

December 21, 2015

Data Privacy and Cybersecurity

On December 15, the EU institutions finally agreed the text of the new EU data protection law, the General Data Protection Regulation ("GDPR"), completing a process that began in January 2012. The LIBE committee has published the consolidated version of the GDPR text. For the consolidated text please see here.

The GDPR heralds a new era of data protection. It replaces the existing data protection framework, which was based on an EU directive. It also makes major changes to the current order: it enhances existing legal requirements; creates a multitude of new rules; and sets out stiff penalties for organizations that fail to comply — similar to those applied for breaches of EU competition law.

The GDPR will apply directly in all Member States two years after the Council and the European Parliament formally approve the text. This approval is expected in the coming months.

This Covington alert discusses the scope of the GDR, summarizes its key elements, and explains the remaining procedural steps in the months ahead.

"One Continent, One Law" —or Not?

"One continent, one law" — this is a key theme in the European Commission's December 15 press release that announced the political agreement on the GDPR. The GDPR does not quite live up to the hype, however. One of the chief motivations for an EU regulation was to remedy having 28 different Member State laws that currently exist despite having common origins in the EU Data Protection Directive 95/46/EC (the "Directive"). Because it is a regulation, the GDPR will have direct effect. But, in the end, the GDPR allows Member States to adopt divergent approaches in some important areas, including on procuring consent from minors, the handling of human resource and health data, and the treatment of scientific research.

The GDPR also will have a broader territorial reach than the Directive. The Directive applies to non-EU controllers if they process personal data "in the context of the activities" of an establishment in the EU or "make use of equipment" in the EU to process data. The GDPR, however, will apply to controllers *and* processors without an establishment in the EU if their processing activities relate to offering goods or services to data subjects in the Union or to "the monitoring of their behavior."

Main Changes to the Current Regime

The agreed text makes many changes that will affect businesses in all sectors. While the general principles of EU data protection law — such as lawfulness, transparency, purpose limitation, and data minimization — will remain, we describe below the most important changes. We separate them into five categories: substantive principles; enforcement and remedies; accountability; transparency and rights; and international transfers.

Substantive Principles

- **Consent** remains an important legal basis for the processing of personal data. The GDPR continues to make a distinction between "unambiguous" and "explicit" consent, although the difference remains unclear. Unambiguous consent must be made by a statement or "clear affirmative action" of the data subject — pre-ticked boxes do not constitute unambiguous consent. As is the case under the Directive, the GDPR requires that consent be "freely given," but now explains that consent may not be coerced, for instance by making consent for non-essential processing a precondition to entering into an agreement, or where there is a clear imbalance between the controller and the data subject. Consent by children, granted in the context of information society services, will only be valid where the child is 16 or older, unless individual Member States adopt a lower age threshold, down to a minimum of 13.

- The **legitimate interests** of companies continue to be a legal basis to process non-sensitive personal data. The company's interests still have to be balanced against the rights of the individual, but — unlike the Directive — the recitals underline the importance of the reasonable expectations of the individual at the time of collecting data. In practice, this is expected to increase the weight given to the data subjects' interests.

- The **purpose limitation** principle continues to apply, which may have consequences for certain, so-called "big data" initiatives. Personal data can be used for other purposes (without consent), subject to a compatibility test or where required by law. Important exceptions apply for scientific research activities.

- There are also new requirements on **profiling**, also potentially relevant in the "big data" area. Profiling is only allowed in exceptional cases, and can be restricted where profiling has legal consequences or important implications for the individual. In such cases, consent may be required.

- For **special data**, such as data relating to health, race, and religion, the rules broadly remain the same as under the Directive: the processing of such data is prohibited, unless the GDPR otherwise permits it. Member States, however, can adopt stricter restrictions on the processing of special data than those appearing in the GDPR.

Enforcement and Remedies

- The "**one-stop-shop**" concept originally was intended to simplify matters by allowing companies to interact with only one data protection authority ("DPA") — renamed Supervisory Authority under the GDPR — across the Union. However, following much debate, this has now become a complex mechanism, involving one "lead" DPA and possibly several "concerned" DPAs. The lead DPA is the DPA with jurisdiction over the controller or processor's "main establishment." Concerned DPAs can intervene and refer the lead DPA's decisions to the European Data Protection Board (EDPB). In these cases, the Board will assess the issue and make a binding decision.

- One of the most contentious and revolutionary changes concerns **sanctions**. Different tiers for fines are set out. For some violations (e.g., violation of record keeping obligations), DPAs may impose fines of up to the greater of 2 percent of a company's annual global turnover or 10 million EUR. For other offences (e.g., violation of data subject rights), fines may rise to as high as 4 percent or 20 million EUR — whichever is greater.

- In contrast to the Directive, DPAs' enforcement powers will be harmonized and DPAs will have the power to impose administrative fines.

- The GDPR also reinforces rights to lodge **complaints** with a DPA and strengthens **legal remedies**. The GDPR explicitly allows individuals to seek legal remedies against DPAs (for example, when a DPA does not deal with a complaint), as well as controllers and, for the first time, processors.

- Processors and controllers are **jointly liable** for damages caused by their processing activities.

- The GDPR appears to pave the way for **class actions**, as it allows organizations to claim compensation on behalf of data subjects, even without an explicit mandate to do so. The practical effect of this will vary significantly between EU countries, however, as such claims may only be brought "if provided for by Member State law."

- The **EDPB** will replace the current Article 29 Data Protection Working Party. The EDPB will have broader powers than the Article 29 Working Party as it will be able to adopt binding decisions. Significantly, it will play a vital role in the one-stop-shop mechanism.

Accountability

- The GDPR continues to distinguish between controllers and processors. The controller essentially remains the entity that alone or jointly with others determines why and how personal data is processed, whereas the processor continues to be the entity that processes personal data on the controller's behalf. However, under the GDPR, controllers are now explicitly required to "demonstrate compliance" with the data protection principles. The GDPR refers to tools to help demonstrate compliance, such as **codes of conduct** or a **certification**. Codes of conduct will be developed by industry and approved by DPAs, whereas certifications will be granted by certification bodies, DPAs, or the EDPB.

- Controllers must notify the DPA of a **data breach** "without undue delay and, where feasible, no later than 72 hours after having become aware of it," unless the breach is "unlikely to result in a risk for the rights and freedoms of individuals." Controllers must notify data subjects of a breach where it creates a "high risk" to the rights and freedoms of individuals, although exceptions can apply.

- This new data breach obligation is in addition to the existing requirement to ensure the **security** of data. The GDPR lists possible security measures, specifying that the appropriate measure depends on the risks associated with the processing.

- Data **processors** now have direct, statutory — instead of merely contractual — obligations. These extend to implementation of technical and organizational measures and include the obligation to notify controllers of data breaches.

- Companies must appoint a Data Protection Officer (**DPO**) when their core activities involve monitoring data subjects or processing special data on a "large scale." The DPO will have considerable powers and a significant amount of independence from the company he or she represents. Small and medium-sized enterprises ("SMEs") are exempt from this obligation.

- Under new **privacy-by-design** requirements, controllers will need to ensure that future products and services take privacy requirements into account. The text encourages companies to pseudonymize personal data where possible, for instance. Similarly, privacy settings on products should protect data subjects "by default." Privacy settings on products may not make personal data public by default.

- Where processing activities are *likely* to result in a "high risk," controllers must carry out a data protection impact assessment (**DPIA**). The recitals provide some guidance on what constitutes a "high risk," but many questions remain. Here, too, there are exceptions for SMEs. DPAs must be consulted in relation to processing operations that present such a high risk.

- The existing national **notification and authorization** requirements will cease to exist under the GDPR, and will be "replaced" by more elaborate internal record-keeping obligations.

Transparency and Rights

- The GDPR places even greater emphasis on ensuring transparency than the Directive. More specifically, the GDPR contains a more elaborate list of mandatory elements that should appear in data protection **notices**, including the contact details of the organization's DPO (if any), the legal basis that the organization relies upon to process the data, the safeguards applied where data are transferred internationally, and data retention periods.

- The traditional **rights of access, rectification, erasure, and objection** remain largely the same. The GDPR sets out specific timelines for complying with requests from data subjects who exercise their rights — namely, one month, with a possible extension to three months.

- The GDPR introduces an entirely new right, which has been widely criticized, referred to as a **right to data portability**. This grants data subjects the right to receive their personal data from a controller in a "machine-readable format" and to have the data transmitted to another controller, where technically feasible.

- The GDPR establishes a qualified right to erasure, frequently referred to as the "**right to be forgotten**." Data subjects can demand that organizations delete or destroy their data on various grounds, including where retaining the data is no longer necessary or where the data subject objects to the processing of the data and there is no overriding, countervailing interest.

- Data subjects have a **right to restriction**, which means that in some cases, they can demand that the further processing (other than storage) of their data may be suspended, such as when the accuracy of the data is contested.

International Transfers

- The GDPR continues to restrict international transfers of personal data to "non-adequate" countries outside the EU, i.e., third countries that have not yet been deemed "adequate" by the European Commission. The GDPR sets out a more elaborate list of elements that the Commission must take into account when assessing the adequacy of non-EU jurisdictions.

- The GDPR restricts transfers in response to **non-EU judicial or administrative procedures**. This restriction is not as strict as was debated at times during the legislative process. Instead of requiring controllers and processors to notify and obtain approval from DPAs in relation to such requests, the GDPR stipulates that such requests are only enforceable if based on an international agreement, such as a mutual legal assistance treaty. Controllers and processors must still abide by the general transfer rules.

- **Binding Corporate Rules (BCRs)** and **standard contract clauses** (or model clauses) issued by the European Commission remain valid instruments to comply with EU data transfer restrictions. Using these transfer mechanisms should become easier as certain existing authorization requirements have been dropped. In addition, national DPAs will be authorized to issue standard contract clauses. Existing Commission and Member State decisions relating to adequacy and the current Commission standard contract clauses remain valid until revised, replaced, or repealed. Other instruments, such as recognized codes of conduct and seals, may also be used for international transfers. Further, under the GDPR, adequacy determinations may be made with respect to third country territories or specified sectors.

- Transfers can also take place on the basis of the **derogations**, similar to those in the Directive. Interestingly, the GDPR adds "legitimate business interest" as a new derogation. However, the conditions are so stringent, including notification to the DPA, that it may not be used very often in practice.

- Member States are specifically authorized to **restrict transfers** of specific categories of personal data for important reasons of public interest. Such restrictions must serve a public interest and be notified to the European Commission.

What's Next?

The Road to Adoption

The European Parliament and the Council must now formally adopt the text. This is expected to be a rubberstamping exercise introducing few, if any, changes to the text agreed on December 15, although, in theory, further discussions are possible.

On December 17, the Civil Liberties, Justice and Home Affairs (LIBE) committee in the European Parliament, supported the political agreement. As a next step, the EU Member States in the Council have to formally adopt the text as a Common Position. On December 18, the text was approved in a meeting of the Committee of Permanent Representatives (Coreper) almost unanimously with one abstention (see press release here). This confirmation paves the way for formal adoption by the Council, which seems expected in the first few months of 2016.

Following the adoption by the Council, the text will have to be approved by the European Parliament in plenary session. The Parliament's plenary is not formally bound by the earlier LIBE committee's opinion, but is very likely to follow it. According to a Parliament press release (see here), the plenary vote may take place in March or April next year.

Implementation

The GDPR will apply directly in all EU Member States. The GDPR will enter into force 20 days after its publication in the Official Journal of the EU, which is expected in the first half of 2016, shortly after Parliament's plenary vote. After this, there is a two-year transition period before the GDPR will apply.

Companies therefore will need to start to comply with the GDPR during the course of 2018. The implementation phase provides much needed time for companies that will have to implement the necessary processes and policies to comply with the GDPR. This may include the appointment of a DPO, revision of informed consent forms and methods to obtain consent, revision of privacy notices and policies, adoption of data breach procedures, the implementation of privacy impact assessments, and so forth.

During this two-year period, Members States will also have to amend or even repeal some existing legislation and guidance in order to comply with the new GDPR. The European Commission has the power to adopt implementing legislation to specify further detailed rules under the GDPR in limited cases. Examples include the criteria and requirements for certification mechanisms, data protection seals and marks, information to be presented by standardized icons, and procedures for providing such icons. The EDPB may issue guidance on the implementation of appropriate practical measures for compliance with the GDPR, such as guidance on profiling.

In the coming weeks, we will post more detailed blog posts on specific topics of the GDPR on our InsidePrivacy blog.

If you have any questions concerning the material discussed in this alert, please contact the following members of our Data Privacy and Cybersecurity practice group:

Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Monika Kuschewsky	+32 2 549 52 49	mkuschewsky@cov.com
Kristof Van Quathem	+32 2 549 52 36	kvanquathem@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com
Sebastian Vos	+32 20 549 5267	svos@cov.com