COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Global Privacy & Data Protection

January 26, 2012

REFORM OF THE EUROPEAN DATA PROTECTION FRAMEWORK

Following more than two years of consultations and intense speculation in recent weeks, the European Commission yesterday proposed comprehensive measures to reform the European data protection framework, including a proposed new General Data Protection Regulation. The proposed Regulation will now move into the EU legislative process, and will have to be considered by the European Parliament (EP) and the Council (i.e. the Member States) before its adoption.

We currently are analysing the proposed reforms in detail, but it appears that the proposed Regulation largely mirrors earlier leaked drafts. Below, we set out a brief summary of certain key measures, and an overview of next steps in the legislative process:

- One law. The proposed law will take the form of a Regulation that will apply across all EU Member States.

- Application to EU and non-EU companies. In addition to EU based companies, the new Regulation will apply to non-EU companies that either process data of individuals residing in the EU to whom they offer goods or services, or whose activities serve to monitor the behavior of such individuals. This replaces the current "making use of equipment" test with a new "targeting" test.

- "One-stop-shop" for EU data controllers – but not for non-EU controllers. EU data controllers will be supervised by the data protection authority of the Member State where the controller's "main establishment" is based. Non-EU based controllers must designate a representative in one of the Member States where they target data subjects, but it appears that this representative may be addressed by "any supervisory authority".

- Broader concept of "personal data" and new definitions. The definition of "data subject" is expanded to cover anyone who can be identified (directly or indirectly) by the controller directly or "any other natural or legal person". Identification may occur by reference to an "identification number, location data, online identifier" or other factors. The Regulation also introduces a host of new definitions, including ones for "personal data breach", "biometric data", "genetic data", "main establishment", and "child" (defined as any person under the age of 18).

- Data transfers. The existing EU restriction on data transfers to countries that do not offer adequate protection remains in place. However, the use of standard contractual clauses will no longer be subject to prior authorization or approval by data protection authorities. Also, the adoption of binding corporate rules (BCRs) would be made easier, and the regime would be extended to data processors; an entire section is devoted to BCRs. The draft Regulation retains the original derogations for transfers to third countries, such as consent, but adds a new derogation for occasional or limited transfers that are necessary for the legitimate interests of a data controller.

- **Legitimate bases to process data and specific rules on consent.** Similar to the existing rules, lawful processing may be based on several grounds, including consent, and where processing is necessary for the performance of a contract with the data subject, for compliance with a legal obligation to which the controller is subject, and for the purposes of the legitimate interests of a controller. The draft law now contains a stand-alone section on consent, however, which is defined as any "freely given specific, informed and explicit indication of will". Consent cannot be used as a legal basis for processing personal data where "there is a clear imbalance between the data subject and the controller", and controllers will have the burden of proving that individuals have consented to processing. Further, consent will not provide a valid legal ground "where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment".

- **Children.** The processing of personal data of a child below the age of 13 years shall only be lawful if consent is given or authorised by the child's parent or custodian. Controllers will have to make reasonable efforts to obtain verifiable consent, "taking into consideration available technology".

- **New rights for individuals.** The draft contains a new "right to be forgotten" that imposes a specific obligation on a controller to erase certain data, and to take steps to erase links to that data where the controller has made the data public. A new data portability right will enable data subjects to obtain a copy of their data from a data controller in a format that "is commonly used" and "allows for further use by the data subject". Individuals also will have the right to transfer certain data in a format that can be used in a different service. The Commission reserves the right to specify the electronic format and technical standards to enable such transmission.

- **Breach notification.** The draft Regulation, as was expected, introduces a comprehensive breach notification regime. It specifies that data controllers must notify any data breach to the supervisory authority "without undue delay and, where feasible, within 24 hours". Controllers also must notify individuals whose personal data could be "adversely affected" -- e.g., if it "could result in identity theft or fraud, physical harm, significant humiliation or damage to reputation" -- without undue delay, unless the controller can demonstrate, to the satisfaction of the supervisory authority, that they have implemented appropriate technological protection measures.

- **Mandatory Data Protection Officer.** Organizations employing 250 persons or more must designate a data protection officer.

- **Sanctions.** The draft Regulation contains an elaborate section on administrative sanctions. Mirroring sanctions for violations of EU competition law, each competent authority would now have the power to impose administrative sanctions and to tailor these sanctions according to a company's annual worldwide turnover. For certain types of intentional or negligent violations, supervisory authorities will be able to impose fines of between 250,000 and 1,000,000 Euros, or up to 2% of an enterprise's annual worldwide turnover.

- **Legislative Process.** As noted, the EP and Council must approve the Commission's proposal before it is adopted.

    - The first step in the EP will be to identify the Parliamentary committee or committees responsible for reviewing the proposal. Importantly, under recent EP rules, it is possible for the EP to appoint more than one lead committee -- creating both challenges and opportunities for those engaged in advocacy on the proposal. The EP must also choose a "rapporteur" -- i.e. the EP member in the committee who will lead negotiations on the proposal. Both the choice of committees and of rapporteur(s) -will play a significant role in the course of the legislation, influencing what amendments to the proposal are tabled and adopted in the EP, but also how negotiations with the Council over the proposal proceed.

- In the Council, the initial analysis of the proposal will be performed by a Working Group staffed by national officials and experts. The Working Group will collaborate closely with the relevant Ministries in each of the Member States on both the political and technical dimensions of the proposal.

- Both the EP and Council must together reach consensus before the proposal can be adopted. Given the importance of the dossier, we can expect the Council and lead MEPs to engage in these negotiations from an early stage in the process, well before each institution finishes its final review of the proposal. Because of the importance of the issue and its complexity, we can also expect that negotiations will be long and controversial. The EP, pushed by left wing and liberal MEPs, is a strong supporter of far-reaching privacy rights, where many (but not all) Member States may have a more balanced, industry-friendly position. There will no doubt be strong political pressure to reach an agreement in first reading (i.e. after only one review by the Council and the Parliament) -- but even if that proves possible, negotiations will likely run at least 18 months.

If you have any questions concerning the reform of the European data protection framework or the legislative process, please contact the following members of our team:

Daniel Cooper (Data privacy)	+44.(0)20.7067.2020	dcooper@cov.com
Jetty Tielemans (Data privacy)	+32.2.549.5252	htielemans@cov.com
Mark Young (Data privacy)	+44.(0)20.7067.2101	myoung@cov.com
Jean De Ruyt (Government affairs)	+32.2.549.5230	jderuyt@cov.com
Lisa Peets (Government affairs)	+44.(0)20.7067.2031	lpeets@cov.com
Wim van Velzen (Government affairs)	+32.2.549.5230	wvanvelzen@cov.com