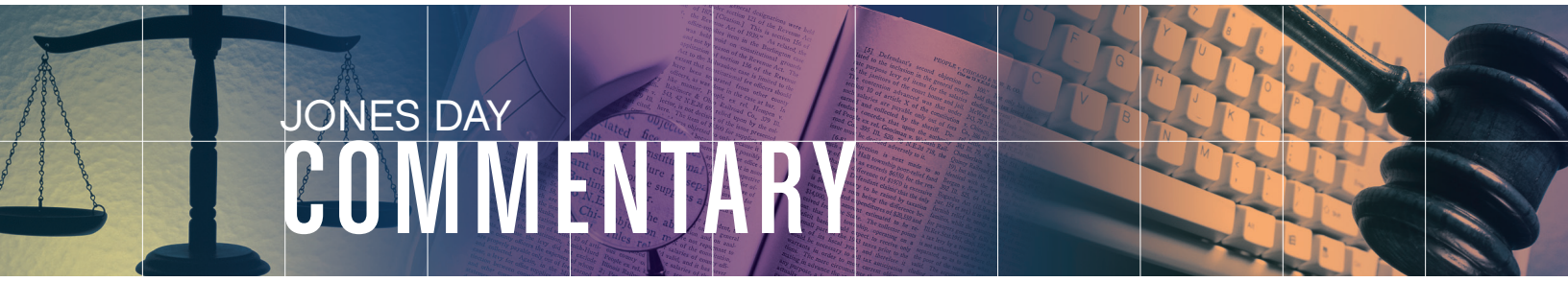
FEBRUARY 2012




# THE EU LAUNCHES INITIATIVE TO REVAMP EU PRIVACY RULES

On January 25, 2012, the European Commission unveiled its draft legislative proposals to revamp privacy rules in the European Union (EU).[1] The proposals are designed to align existing data privacy rules, dating from the 1995 Data Protection Directive ("1995 Directive"), with recent evolutions in technology, such as the rise of a global internet, cloud computing, social networking sites, smart cards, and the so-called "internet of things."

The proposals consist of a new draft regulation ("Draft Regulation") and a new draft directive ("Draft Directive"). These proposals are accompanied by a regulatory impact assessment, a report, a draft communication and various press documents and tools. The Draft Regulation addresses data protection by companies doing business in the EU's internal market, while the Draft Directive concerns data protection in the exchange of information between EU Member State police and judicial authorities in the fight against serious crime.

## ANTITRUST-LIKE FINES

The most salient change is the introduction of a system of fines for breaches of data protection rules by individuals or enterprises. This proposed system resembles, albeit with much lower thresholds, the current penalty framework for antitrust violations.

For businesses, the following fines are contemplated:

- Fines of up to 0.5 percent of the annual worldwide turnover (which would generally mean worldwide annual gross sales revenue) would apply for failure to establish adequate mechanisms for responding to information requests by data subjects, or if a response to such request is not timely or free of charge.
- Fines of up to 1 percent of annual worldwide turnover may apply when "anyone who intentionally or negligently" fails to (i) fully respond

1 See http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

to information requests by data subjects, (ii) rectify mistakes, (iii) comply with the "right to be forgotten," (iv) obstruct data portability, (v) sufficiently determine co-responsibility with co-controllers, (vi) maintain sufficient documentation on processing operations, or (vii) adhere to rules for sensitive data.

- Fines of up to 2 percent of annual worldwide turnover are contemplated in several cases, including (i) illegal processing of data and sensitive data, (ii) failure to appoint a data protection officer or, for undertakings located outside the EU, a representative within the EU, (iii) lack of appropriate measures to comply with the privacy "by default" and "by design" principles (as further explained below), (iv) failure to provide notice of a data breach in a timely and/or complete manner, (v) failure to perform an impact assessment and obtain prior authorization where required, (vi) failure to cooperate with data protection authorities ("DPA"), (vii) breach of rules on international data transfers, and (viii) failure to comply with professional secrecy rules.

The above-mentioned fine levels are maximum amounts, and the extent to which turnover will also be used in practice as a matrix to calculate actual fines remains to be seen. The Draft Regulation provides only for criteria that must be taken into consideration for setting fines, such as the nature, gravity, and duration of the breach, intent, recidivism, and cooperation, but it does not actually establish fining guidelines.

## EXTENDED SCOPE OF PRIVACY RULES

The proposals also extend the scope of privacy rules, both materially and territorially.

Materially, the Draft Regulation increases the protection afforded to data subjects by expressly including within the scope of personal data all data that can be identified by reference to location data and online identifiers. Sensitive data requiring specific protection now also include criminal records and genetic data. Furthermore, obligations previously applicable only to data controllers (*e.g.*, data owners) are now also applicable to data processors (*e.g.*, service providers). For instance, service providers that process personal data on behalf of the controller, such as many cloud computing companies, will have direct obligations under the Draft Regulation. Currently, controllers are required to impose data protection requirements on processors. The Draft Regulation also confers joint-controller status on a processor that processes data beyond the controller's instructions.

Territorially, the Draft Regulation extends the application of data protection rules to undertakings not established in the EU if (i) the data originates from persons residing in the EU, and (ii) the processing activities relate either to the offering of goods or services in the EU or the monitoring of the person's behavior in the EU. Such undertakings must now also designate a representative within the EU.

## OPT-IN

Consent remains the keystone of the framework but is now more strictly defined. According to the 1995 Directive, the data subject should "unambiguously" give his consent prior to data processing. Consent now needs to be explicit, *i.e.*, given either by a statement or by clear affirmative action. The Draft Regulation thus sanctifies the "opt-in" system. The consent of children below the age of 13 will now entail verifiable parental consent.

## ONE-STOP SHOP

Depending on the countries where they do business, companies can currently be subject to up to 27 sets of different rules and DPAs. The Draft Regulation establishes the country of origin principle, whereby the applicable law and the competent DPA will be that of the country where the business has its main place of establishment, *i.e.*, for the controller, this is essentially the place in the EU where the main decisions on data processing are made; for the processor, this is the place of central administration within the EU.

However, there are limitations to the one-stop-shop principle, because the Draft Regulation allows data subject and data protection associations to (i) lodge complaints to the DPA in their country, and (ii) bring proceedings against a controller or processor before the courts of the Member State where the data subject has his habitual residence.

## ABOLITION OF THE NOTIFICATION PROCEDURES, EXCEPT FOR DATA BREACHES

The current system of systematic notifications to the DPA of automatic data processing is proposed to be eliminated. Instead, companies will be responsible for self-assessing their practices based on (i) the internal appointment, within medium and large businesses, of a data protection officer to monitor compliance, (ii) the maintenance of documentation of all processing operations, to be available on request to the DPA, and (iii) impact assessments and prior approval of the DPAs for certain processing, such as video surveillance and large-scale filing systems on children, genetic data, or biometric data.

The Draft Regulation also contemplates requiring companies to provide notice of any data breach to (i) the DPA as soon as possible, and where feasible within 24 hours, and (ii) data subjects affected by the breach without undue delay.

## STREAMLINING INTERNATIONAL DATA TRANSFERS

The Draft Regulation first clarifies that the Commission alone shall adopt adequacy decisions (*i.e.*, determinations that the country of destination affords adequate data protection), allowing the free flow of information. The Draft Regulation also formalizes the practice of Binding Corporate Rules ("BCRs"), as developed by the Article 29 working party. BCRs are personal data protection policies, adhered to voluntarily by controllers to transfer data within a group of companies.

The Draft Regulation aims at increasing BCR efficiency by simplifying the process of DPA approval of BCRs and by extending their use to data processors. Finally, a new derogation is introduced based on the controller's or processor's legitimate interest, but only if the transfer is not frequent or massive, and only after assessing and documenting the circumstances of that transfer.

## RIGHT TO BE "FORGOTTEN," PRIVACY BY DEFAULT, PRIVACY BY DESIGN, AND DATA PORTABILITY

The draft Regulation introduces several new concepts.

First, the "right to be forgotten" strengthens the possibility to delete incomplete or inaccurate data by allowing each data subject to request a controller to delete any stored personal data and to stop any further dissemination of such data. Where the controller has made the data public, this would mean taking all reasonable steps toward removal of any link, copy, or replication of such data.

Second, under "privacy by design," appropriate technical and organizational measures and procedures shall be implemented, by the time of the determination of the means of processing, in order to guarantee the protection of the rights of data subjects.

Third, "privacy by default" implies that privacy-friendly default settings will be the norm under the Draft Regulation.

Fourth, "data portability" triggers a right to transfer data from one electronic processing system to another, without hindrance from the controller. If asked by the data subject, the data controller must provide a copy of data undergoing processing in an electronic and structured format that is commonly used, allowing for further use by the data subject.

For all of the above concepts, the Commission shall have the power to adopt secondary legislation to detail these specific obligations.

## NEXT STEPS

The proposed draft legislation will now be discussed in the European Parliament and the European Council, both of which may amend the text prior to its final adoption. The duration of the legislative process will depend on the ability to find a common position, but it is not expected to be finalized before 2013.

## LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.


**Laurent De Muyter**
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

**Alexandre Verheyden**
Brussels
+32.2.645.15.09
averheyden@jonesday.com


## ADDITIONAL CONTACTS


France
**Emmanuelle Rivez**
Paris
+33.1.56.59.39.39
earivez@jonesday.com

Germany
**Dr. Undine von Diemar**
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Italy
**Stefano Macchi di Cellere**
Milan
+39.02.7645.4001
smacchi@jonesday.com

**Afra Mantoni**
Milan
+39.02.7645.4001
amantoni@jonesday.com

United Kingdom
**Jonathon Little**
London
+44.20.7039.5224
jrlittle@jonesday.com

United States
**Kevin D. Lyles**
Columbus
+1.614.281.3821
kdlyles@jonesday.com

**Mauricio F. Paez**
New York
+1.212.326.7889
mfpaez@jonesday.com