



European Commission proposes reforms to Data Protection Law

On January 25th, 2012, the European Union introduced its much anticipated reforms to the 1995 Data Protection Directive. The proposals offered by Commissioner Viviane Reding, Commissioner for Justice, Fundamental Rights and Citizenship, are some of the most sweeping changes to data protection and online privacy ever made. In addition to working to create a digital single market, as proposed in the 2010 Digital Agenda for Europe, the rules create new consent mechanisms for both adults and children, increased individual control over personal data and a right to be forgotten for all. .

Within the European Union (EU), Article 8 of the Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the European Union provide all citizens with the right to the protection of their personal data. This includes the requirement of informed consent for collection and processing and independent oversight of such matters by individual Member States. Decreasing consumer confidence in data protection, taken in conjunction with high costs for businesses operating throughout the Union, has spurred the European Commission to take action. The reforms to the current framework are designed to standardize data protection throughout the 27 Member States, to simplify and encourage compliance and importantly to save companies over €2.3 billion a year. In order to meet their aims, the Commission has proposed both a Regulation and a Directive. The Regulation would be directly effective and would set out the general data protection framework, while the Directive, requiring national incorporation, would regulate the processing of personal data by judicial authorities. Commissioner Reding hopes that through these measures, businesses will save money, consumers will regain trust in online markets and young people will be afforded increased protection.

In recent years the EU has demonstrated a staunch commitment to child Internet safety. Most recently, Commissioner Kroes, Commissioner for the Digital Agenda, created the CEO Coalition to make the Internet a better place for kids. However, the revisions proposed in this review pre-empt the Coalition with changes to consent mechanisms for children under 13, simplification of privacy policies for all children under 18, and the creation of a 'right to be forgotten.' Throughout the Regulation, there is an overarching objective of improving children's online privacy and promoting their reputation management.

Article 8 of the proposed Regulation amends the provisions for obtaining consent for the processing of children's data. Currently, in order to collect this personal data, companies must obtain parental consent for all minors under 13. This brings the EU in line with the US position under the Children's Online Privacy Protection Act. While this requirement was already often complied with, given the global nature of the Internet and the multi-national companies that operate therein, this article formalizes it. The Regulation also provides for strict sanctions. Should companies violate this law, they may be fined €1 million or up to 2% of their global turnover. The legislative instrument dictates that all communication aimed at minors must be clear and in plain language, with particular regard paid to the data subject. This will ensure that young people can understand the implications of entering their data, the reason it is needed, and the protection that it is afforded.

Article 17 of the Regulation, the 'right to be forgotten and to erasure,' has prompted the most debate in Europe and in the United States. The article states that all users should have the right to request that their personal data be deleted. Although a requirement of data minimization already existed, the new law would enshrine it as a right. Explanations from the Commission state that the 'right to be forgotten' comes as part of a three-fold regime. Firstly, a baseline that the minimum amount of data is meant to be collected and processed. Secondly, that the privacy controls for all users are automatically set to the most private, also known as 'privacy by default,' and finally that upon request, and in the absence of legitimate reasons to maintain it, all personal data belonging to an individual is deleted completely. There are derogations where deleting the data would interfere with free expression or public safety.

The Regulation goes further and states that when the data has been made public, the service who has received the data deletion request must take all reasonable steps to ensure that third parties are made aware of the deletion request and that they cease processing of that information. This puts a tremendous burden on websites who will be punished by a fine of €500,000, or up to 1% of global turnover, for failure to act. [Critics](#) of the article have alleged that it is impractical and overly ambitious, and that small businesses will be unable to comply with deletion requests, especially when it comes to their responsibility for third party processing of data.

In addition to 'privacy by default,' the Commission has recommended a system of 'privacy by design,' i.e. a standard by which companies build in privacy settings to their products. There is a requirement that allows for all users to be able to transfer their data easily between services and, in light of recent high-profile events involving data breaches, the new law prescribes that in cases of breach the data protection authority must be notified immediately, within 24 hours, and the individuals concerned should be informed as soon as possible and without undue delay.

To the distinct advantage of the business community, the reforms propose a single set of rules that will be valid across the EU. Companies will no longer be required to comply with individual states' data protection rules. They will instead work with the data protection authority in the country in which they have their main establishment, and compliance will be assumed throughout the Union. The Regulation also details that the rules apply not only to those who are processing personal data within the Union, but also to those who are working outside the borders but who are collecting data from EU citizens for the purposes of offering goods or services or monitoring behaviors. This massively extends the geographic reach and impact of the reforms.

The global nature of the Internet means that while the EU may be changing the rules and requiring compliance by all companies doing business within its borders other countries will need to decide whether to take action and if so, whether to legislate or promote industry guidelines and responsibility. In a nation that has previously relied more on the self-regulatory approach, the United States is now pushing ahead with its recommendations to amend the current

privacy framework. It is expected that the White House will publish its position shortly. Having just completed a review of the Children's Online Privacy Protection Rule in 2011, it is also likely that the Federal Trade Commission will release a privacy report later in 2012. While it is expected that the EU and the United States will set global standards on this front, other countries are also amending their legislation to confront the changing nature of online sharing. India has proposed creating a formal 'right to privacy,' and China has plans to limit the transferring of personal information between companies without consent. Both Asian countries will shortly have more people online than the United States and Europe have citizens, so reforms taken here should be watched closely.

The European Commission has worked diligently to restore trust and put individuals back in control of their data. However, the concern is that with this Regulation and Directive they have become overly prescriptive. Instead of making it simpler to operate a business within the EU, they have created obstacles with increased burdens and stricter sanctions for non-satisfaction of duties. There is a commitment to child safety and an acknowledgment that those under 18 deserve specific protections tailored to their understanding of risks and consequences, however education may be more of a solution than regulation.

The proposals will now be examined by the European Parliament and the 27 Member States; the Commission has indicated its intention to pass this legislation before the end of 2012, with it becoming effective 2 years after they have been adopted. For more information please see FOSI's [Global Resource and Information Directory](#) or contact emorris@fosi.org

About FOSI

The Family Online Safety Institute is an international, non-profit organization which works to make the online world safer for kids and their families. FOSI convenes leaders in industry, government and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.