The EU General Data Protection Regulation: are you ready?

Intellectual Property and Technology News

2 DEC 2015
By: Carol A. F. Umhoefer

In 1995, the EU Data Protection Directive established the first-ever legal framework for personal data protection across multiple countries. The Directive has since shaped how the EU member states − and countries across the world − look at individuals' privacy rights in their personal data.

In the coming months, we will witness what may be the most important event to date in the short history of personal data protection law: the EU will adopt the EU General Data Protection Regulation, or GDPR, resetting the pace of reform and raising the bar for data protection in the EU and across the world.

The path to reform has been long. The first consultations on the GDPR opened in 2009. The European Commission, European Parliament and European Council are currently negotiating the final terms; the final version is expected by early 2016; and the GDPR could be effective as early as 2017.

The GDPR will replace the Directive in its entirety. Intended to harmonize the data protection regime across all of the EU, the GDPR will be directly applicable to member states, eliminating the need for national data protection laws in the 28 EU member states.

Here's a quick look at just a few of the many significant changes:

TERRITORIAL APPLICATION OF EU DATA PROTECTION LAW

Since 1995, EU data protection laws have applied whenever a data controller (an entity determining how and why personal data is processed) is established in the EU, or is established outside the EU but using means of processing personal data (such as servers) in the EU.

The GDPR will adopt a consumer law approach to application of EU data protection law: businesses will be subject to the GDPR if they target EU consumers, even if the businesses are not established in the EU and do not use servers in the EU to process data. As a result, it is possible that the simple act of selling a product to an EU resident (even without actively targeting the EU market) and processing that one resident's data during the sale, will be enough to trigger oversight by the GDPR.

ADMINISTRATIVE FINES

The maximum fines for violations of data protection law will increase dramatically under the GDPR.

Though the terms are not yet final, both the European Commission and the European Council have proposed that any relevant authority (typically a national authority) may impose a fine up to €1 million or up to 2 percent of yearly worldwide revenues. The Parliament's version of the draft GDPR increased the maximum fine to €100 million, or up to 5 percent of yearly worldwide revenues, whichever is higher.

DATA SECURITY BREACH NOTIFICATION

The GDPR will likely require notification of security breaches under certain specified circumstances and within a predetermined period. Among the circumstances currently under discussion: breaches that could create a risk of discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, or loss of confidentiality of data protected by professional secrecy. Other scenarios that could lead to significant economic or social disadvantage are also being considered for the notification requirement.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The GDPR will require Data Protection Impact Assessments (DPIA), but the situations in which they are mandated are still under review. A DPIA is a documented assessment of the risks a particular personal data processing operation may raise for the privacy of individuals (such as profiling that forms the basis of a decision producing legal effects).

PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

Privacy by design is the notion that a product or service can be conceived from the outset to ensure a certain level of privacy for an individual's personal data. Privacy by default is just that − products and services should be default-set to ensure privacy of personal data.

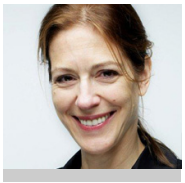
The GDPR will include obligations for data controllers to adopt privacy by design and privacy by default principles. While there is no agreement on the details yet, the European Parliament's proposed version goes the farthest, providing that any data controller shall ensure that, by default, the only personal data processed is the data necessary for each specific part of the processing, and that the personal data is not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of volume of data and duration of its storage. In particular, the controller will need to implement mechanisms to ensure that an indefinite number of people cannot access consumers' personal data and that individuals are able to control the dissemination of their personal data.

You may also enjoy our brief look at what the Directive means for US companies.

For further information regarding the EU GDPR, please email us at and a member of our Data Protection, Privacy and Security team will respond to you shortly.

AUTHORS

Carol A. F. Umhoefer



Partner
Miami | T: +1 305 423 8500
