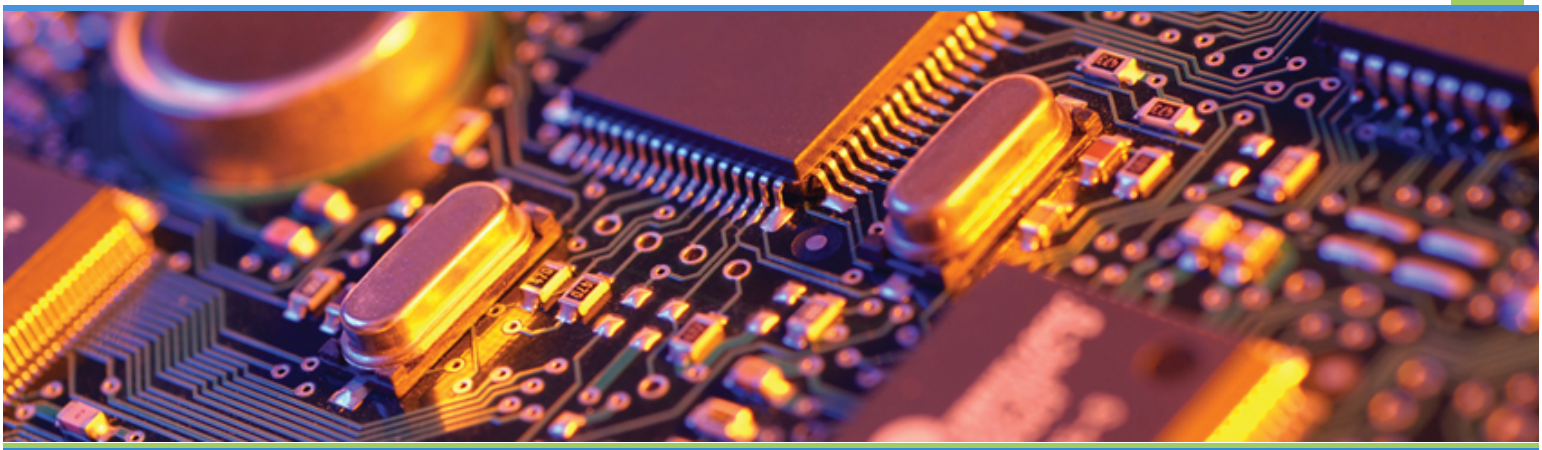
GT GreenbergTraurig



Privacy & Data Security | Alert

December 2015

Important Data Protection Update: Agreement Reached on New Data Protection Regulation in Europe

We have seen dramatic data protection developments in the European Union over the last week! On Dec. 15, 2015, the European Parliament, the European Council and the European Commission agreed on the final wording of the new General Data Protection Regulation ("GDPR"). The GDRP sets forth a number of new requirements that apply to data "controllers" (the entity responsible for determining the nature and means of how personal data is collected and processed) and data "processors" (an entity that performs services for the controller according to directions provided by the controller).

Next Steps

As a formality, a vote on the drafts will be taken by the European Parliament early next year. Two years after its publication in the Official Journal, the GDPR will then be fully and directly applicable throughout the EU, without any necessity for the EU Member States to implement the Regulation into national laws. For businesses with offices throughout Europe, this will mean an end to multiple supervisory authorities with conflicting regulations and piecemeal regulatory frameworks. Instead, there will be "one continent, one law." There are only a few provisions that the Member States may implement into national law within this two years' timeframe.

What will change?

The official final text of the GDPR is over 200 pages and is not yet publicly available, but we have learned the following key points from credible sources:

1. One-stop-shop enforcement: New powers will be provided to national data protection authorities. Complaints

and infringements with regard to cross-border processing of personal data will be dealt with by a lead national authority in the Member State where the main establishment of the controller or processor is located.

2. Consent: Where processing of personal data is based on consent, the controller will be required to be able to demonstrate that such consent was given. Thus, "implied consent" appears to practically be ruled out. Furthermore, the GDPR also will require controllers to allow individuals to withdraw their consent easily and at any time. The GDPR also provides for rules to assess whether consent actually was given freely. For example, consideration will be given to whether the performance of a contract was made conditional on the consent without the relevant data being necessary for such performance. Without consent, the processing will be deemed lawful if the data is processed on a legitimate basis laid down in the GDPR or other law, such as the necessity for compliance with legal obligations to which the controller is subject, or the necessity for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject before entering into a contract.

   For eCommerce, social media and/or content/information service providers to process personal data of persons younger than 16 years, the consent of the child's parent or custodian is required. However, the Regulation allows Member States to lower this age limit to 13 years.

3. Breach notification: In case of a data breach, the controller will be required to notify its supervisory authority of such breach 'without undue delay' and, if feasible, not later than 72 hours, unless it is unlikely that the breach will cause harm to the rights and freedoms of individuals. If the data breach is likely to result in a high risk of harm to the rights and freedoms of individuals, the controller also will be required to inform the data subjects without undue delay, unless one of the exemptions stated in the GDPR applies. However, the Regulation does not define "risk" or provide guidelines about when a risk is "unlikely" or "highly likely", nor does it address conflicts with confidentiality obligations under non-EU laws.

4. Fines: Fines for violations of the basic GDPR principles for data processing (including but not limited to inability to demonstrate that consent was obtained) as well as non-compliance with certain orders of the supervisory authority, can be up to the higher of €20 million ($21.5 million) or 4% of the total worldwide annual turnover of the preceding financial year. For other violations, fines can be up to the higher of €10 million ($10.8 million) or 2% of such turnover.

5. Intra-Group Data Transfers: Under the GDPR affiliates of a controller will be deemed third parties for purposes of data protection law, and a transfer of personal data to an affiliate will be subject to the same requirements as a transfer to an unrelated entity.

6. Right to be forgotten: Data subjects will have the right to request the deletion of personal data in a variety of situations, including but not limited data that was processed when the data subject was still a minor with the parent's approval. Notably, the right is absolute and applies even if the data has been made public already.

7. Data protection by design and by default: At the time when the means for processing personal data are determined, and also at the time when the data is processed, controllers will be required to implement technical and organisational measures, such as pseudonymisation, that are designed to implement data protection principles (e.g., data minimisation). Furthermore, controllers will have to implement appropriate technical and organisational measures to ensure that, by default, only the personal data that is necessary for each specific

purpose is processed. This means that the specific purpose will determine the amount of data collected, the extent of its processing, the time period for its storage and accessibility, etc. Consequently, by default, controllers will not be permitted to make personal data accessible to an indefinite number of individuals without obtaining the individual's consent.

8. Transfer of data outside the EU: The GDPR includes a number of additional 'appropriate safeguards' for the transfer of personal data to a third country besides the options that are currently available. In addition to (i) the binding corporate rules and (ii) the standard data protection clauses adopted by the Commission, it will be possible to rely on (iii) standard data protection clauses that are issued by national supervisory authorities and approved by the Commission, (iv) approved codes of conduct, (v) approved certification mechanisms, and (vi) legally binding and enforceable instruments between public authorities or bodies. However, it remains to be seen whether such measures can fill the gap that was created by the ECJ's invalidation of the Safe Harbor on Oct. 6, 2015. [Click here for GT's alert about that development]

9. DPOs: Many private and public sector data controllers or data processors will have to appoint a data protection officer. This requirement will apply to all organisations whose core activity consists of (i) the regular and systematic monitoring of data subjects on a large scale or (ii) the processing of special categories of personal data, or data relating to criminal convictions and offences on a large scale.

What's next?

Once the 200 pages of full text are public, there will no doubt be more discussion on the meaning and practical implications. Greenberg Traurig's Privacy and Data Security attorneys will follow up on any developments and provide analysis and practical advice to keep you informed.

This *GT Alert* was prepared by **Viola Bensinger**. Questions about this information can be directed to:

> Ian C. Ballon | +1 650.289.7881 | ballon@gtlaw.com
> Viola Bensinger| +49 (0) 30 700 171 150 | viola.bensinger@gtlaw.com
> Luke Dixon | +44 (0) 203 349 8756 | dixonl@gtlaw.com
> Françoise Gilbert | +1 650.804.1235 | gilbertf@gtlaw.com
> Lori S. Nugent | +1 214.665.3630 | nugentl@gtlaw.com
> Radboud Ribbert | +31 (0) 20 301 7333 | ribbertr@eu.gtlaw.com
> Elizabeth C. Rogers | +1 512.320.7256 | rogerse@gtlaw.com
> Alan N. Sutin | +1 212. 801.9286 | sutina@gtlaw.com
> Any member of the Privacy and Data Security Practice
> Or your Greenberg Traurig attorney

Albany
+1 518.689.1400

Amsterdam
+ 31 20 301 7300

Atlanta
+1 678.553.2100

Austin
+1 512.320.7200

Berlin¬
+49 (0) 30 700 171 100

Berlin-GT Restructuring¯
+49 (0) 30 700 171 100

Boca Raton
+1 561.955.7600

Boston
+1 617.310.6000

Chicago
+1 312.456.8400

Dallas
+1 214.665.3600

Delaware
+1 302.661.7000

Denver
+1 303.572.6500

Fort Lauderdale
+1 954.765.0500

Houston
+1 713.374.3500

Las Vegas
+1 702.792.3773

London*
+44 (0)203 349 8700

Los Angeles
+1 310.586.7700

Mexico City+
+52 55 5029.0000

Miami
+1 305.579.0500

New Jersey
+1 973.360.7900

New York
+1 212.801.9200

Northern Virginia
+1 703.749.1300

Orange County
+1 949.732.6500

Orlando
+1 407.420.1000

Philadelphia
+1 215.988.7800

Phoenix
+1 602.445.8000

Sacramento
+1 916.442.1111

San Francisco
+1 415.655.1300

Seoul∞
+1 82-2-369-1000

Shanghai
+86 21 6391 6633

Silicon Valley
+1 650.328.8500

Tallahassee
+1 850.222.6891

Tampa
+1 813.318.5700

Tel Aviv^
+03.636.6000

Tokyo¤
+81 (0)3 3216 7211

Warsaw~
+48 22 690 6100

Washington, D.C.
+1 202.331.3100

Westchester County
+1 914.286.2900

West Palm Beach
+1 561.650.7900