The GDPR: A Broad-Reaching Game Changer

Passed on April 26, 2016, the General Data Protection Regulation (GDPR) is set to take effect on **May 25, 2018**. Replacing the 1995 Data Protection Directive, the GDPR contains key changes that affect businesses throughout the world,[1] including U.S. Companies. Understanding these new regulations is essential to maintaining compliance and avoiding harsh penalties.

The GDPR is an EU regulation concerning data privacy. In the United States, data privacy laws tend to be segmented to specific fields (FERPA, HIPPA, etc.…). However, the European Union considers data privacy to be a fundamental human right and thus applies data privacy laws consistently across the board.[2] The main purpose of this regulation is to protect "personal data" in European Union member countries or countries where "personal data" originating in the EU is stored, processed or retained. This is important as it greatly expands who is regulated in comparison to its predecessor directive.

In this context, personal data is defined as "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address".[3] Note that the inclusion of information as simple as email addresses, login-information, or computer IP addresses means that the GDPR can apply to many U.S. corporations simply through the course of normal business activities.

Companies are specifically required to comply with the GDPR if they fit any of three specific criteria. The GDPR applies to any company that maintains an "establishment" in an EU member nation, whether or not data collection or processing occurs there.[4] Establishment generally means "any real and effective activity – even a minimal one" through "stable arrangements" in the EU.[5] Secondly, the GDPR applies "where the processing activities are related to offering goods or services to data subjects in the Union." This provision even includes goods and services that are free.[6] Moreover, the bar to "offering goods" is low and can be as simple as the specific language, shipping options, or currencies being that of an EU member. Lastly, the GDPR applies to a company "if it processes the personal data of data subjects in the EU and that processing is related to the 'monitoring' in the EU of the 'behavior' of data subjects as their behavior takes place within

[1] http://www.clarkhill.com/uploads/medium/resource/2628/Clark_Hill_-_GDPR_Brief.pdf
[2] http://fra.europa.eu/en/news/2017/strengthening-modern-human-right-data-protection-eu
[3] http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
[4] Art. 3, ¶ 1, GDPR.
[5] https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/11--guide-to-the-gdpr--material-and-territorial-scope.pdf?la=en
[6] Art. 3, ¶ 2(a), GDPR.

the EU". In this context, "monitoring" includes the use of cookies and other information frequently used by advertisers to track and recommend products to consumers.[7]

The GDPR can alternatively come into force against U.S. corporations who do not collect data but instead import/export data from the EU. Under the GDPR, in language mostly unchanged from the 1995 directive, data can only be exported to countries that are deemed to have equivalent or stronger data protection laws than the EU. However, **the U.S. is not considered one of these countries and U.S. corporations must be able provide adequate assurances that data will be handled in accordance with the GDPR**. An exception to this is U.S. companies under the authority of the Federal Trade Commission or Department of Transportation that have signed on to the 2016 EU-U.S. Privacy Shield framework. The Privacy Shield, the successor of the Safe Harbor Program struck down in 2015 after the Edward Snowden leaks,[8] allows companies that self-certify compliance to receive EU personal data as if they were in a country approved by the commission. Companies that are unable or do not wish to join the Privacy Shield program have alternatives. The European Commission allows companies to use pre-approved standard contractual clauses,[9] binding corporate rules,[10] or codes of conduct that have been approved by the European Commission or independent state supervisory authorities. Importantly, companies are not only responsible for their own exports and compliance but also for any "onward transfers" and the compliance of any company down the chain.[11]While companies can share data protected by the GDPR, they must ensure that said company or their contract meets the criteria above.

Knowing these broad categories for which a U.S. company can be subject to the GDPR, examining what must be met for compliance is essential. Penalties for the GDPR are extreme, failure to comply can result in fines of up to 4% of global revenue or 20,000,000 euros, whichever is greater,[12] and direct liability to anyone impacted by mishandled data.

The GDPR has two different sets of requirements depending on a company's classification as either a data "controller" or data "processor". A data controller "acting alone or together with others, determines the purposes and means of the processing of personal data".[13]A data processor "processes personal data on behalf of the controller".[14] While not all encompassing, important requirements for data controllers include: establishing when privacy notices are required,

---

[7] ART. 3, ¶ 2(b) GDPR.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362
https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/

[9] Art. 46, ¶ 2(d), GDPR.

[10] Arts. 46, ¶ 2(b) & 47, GDPR.

[11] Section 4 https://wp.nyu.edu/compliance_enforcement/2017/12/11/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/

[12] Art. 83, ¶ 6, GDPR.

[13] Art. 4, ¶ 7, GDPR.

[14] Art. 4, ¶ 8, GDPR.

including insufficiency of pre-checked boxes which are common practice in the U.S; placing restrictions on choosing data processor; establishing data breach notification timelines and individual rights; recordkeeping; and appointing a data protection officer.[15] This differs slightly for data processors who have regulations on issues such as data breach notification, data security, recordkeeping, and subprocessing, but not many of the restrictions concerning privacy and the actual notices themselves.[16]

The GDPR updates EU data protection laws to provide a far-reaching jurisdictional range. The data protected includes many data types commonly used by US businesses. Act now, before May 25th, and review the specific controller or data processor regulatory requirements if you believe that your business falls under the GDPR's authority.

Sources:

http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
https://www.itgovernanceusa.com/gdpr-data-export-and-eu-us-privacy-shield
http://www.clarkhill.com/uploads/medium/resource/2628/Clark_Hill_-_GDPR_Brief.pdf
http://www.jonesday.com/files/Publication/1af15508-11e4-496f-8c03-556e05f16907/Presentation/PublicationAttachment/e7deefa8-0d0e-4d9a-8967-76c9d5ca88f5/GDPR%20Guide%2002Feb2018.pdf
https://epic.org/privacy/intl/privacy-shield/
https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/
https://wp.nyu.edu/compliance_enforcement/2017/12/11/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/#_edn13
https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/11--guide-to-the-gdpr--material-and-territorial-scope.pdf?la=en

Max Krauskopf, Global Trade Expertise, March 28th, 2018

[15] Section 2.3 https://wp.nyu.edu/compliance_enforcement/2017/12/11/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/

[16] Section 3 https://wp.nyu.edu/compliance_enforcement/2017/12/11/the-general-data-protection-regulation-a-primer-for-u-s-based-organizations-that-handle-eu-personal-data/