GT GreenbergTraurig

Alert | Cybersecurity, Privacy & Crisis Management

February 2018

The GDPR Deadline Looms: Is Your U.S. Website Ready?

Effective May 25, 2018, the European Union's General Data Protection Regulation (GDPR) imposes sweeping new requirements for many website operators that collect and process information about individuals living in the European Economic Area (EEA). U.S. companies with e-commerce and other web activities reaching persons living in the EEA need to understand GDPR, since penalties for violations can reach the greater of four percent of global revenue or EUR 20 million.

Does GDPR Apply to your U.S.-Based Website Activities?

GDPR is complex. However, there are some key concepts that suggest that the new regulation may apply to U.S. website operators even though they may view their activity as U.S.-based. If any of the following three things is true for a company, it is likely that the GDPR will impose certain legal obligations on that company: (1) it has a physical presence in the EEA; (2) it offers goods or services to persons in the EEA; or (3) it tracks or monitors the behavior of individuals in the EEA, including for purposes of serving targeted advertising or other marketing purposes.

The reach of GDPR is broad but is not unlimited. The mere fact that a U.S.-based website can be accessed in the EEA isn't enough. If the company does not have a physical presence in the EEA, it must be determined whether that company engages in more than incidental contact with EEA residents. Examples of activities which may cause GDPR to apply to a U.S.-based website operator include the following:

- Translating the site into a non-English language spoken in the EEA.
- Using a two-letter country domain of an EEA country (.UK, .FR, .DE, etc.).
- Displaying prices or accepting payment in Euros or other European currencies.
- Shipping products to customers in the EEA.
- Direct email marketing to persons in the EEA.
- Monitoring/tracking the online behavior of EEA residents to serve targeted ads.

Accordingly, operators of U.S.-based websites need to assess the extent to which they are "aiming" their activities at EEA residents to determine if GDPR applies. This is a fact-intensive issue that requires looking at all aspects of how the company interacts with EEA residents online and through related activities such as the operation of call centers or the shipment of goods.

How Are U.S. Companies Responding?

Some U.S. website operators are choosing to avoid the application of GDPR by changing their business practices, for example by refraining from selling to individuals in Europe and blocking European-based IP addresses from being tracked when visiting the site. This approach can make sense if a company has very limited sales or web traffic in Europe. Other operators are separating their Europe-targeted activities into separate, EEA-based websites, and isolating the compliance duties with those sites. This latter approach can make sense if your company has an EEA-based affiliate or maintains separate EEA-based websites for other reasons (such as customs and tax issues). ***Caution***: Transfers of data from a European company to a U.S.-based company can trigger separate concerns under GDPR provisions restricting transfer of personal data out of the EEA unless appropriate safeguards are in place. Still other companies are recognizing that their U.S.-based activities may be covered by GDPR and are starting to take steps to come into compliance. Given the many areas of company operations affected by GDPR, any company planning to comply should start soon to be ready by May 25, 2018.

What Kinds of Things may be Required by GDPR?

As stated above, GDPR is a very complex regulation, but the operator of a U.S.-based website with a U.S.-style privacy policy can consider the items in the chart below as a starting point of compliance measures that may be required for purposes of typical marketing practices. The actual measures required for any particular operator will vary based on the individual operator's data-privacy and security practices and use of personal information for marketing purposes. ***Caution***: The chart below focuses on requirements related to marketing practices; a complete review of the entire GDPR – including internal data security and other requirements – should be done to establish a full and complete list of action items.

No.	Requirement	Steps to Consider
1	Limit data usage to the purpose(s) for which data was collected.	If the use of personal data will go beyond the immediate purpose for which personal data was collected (for example, to complete a sale), the operator generally will likely need to obtain the clear and unambiguous informed consent of the consumer unless (i) it has a "legitimate interest" in the use of such data, or (ii) in the event one of the limited express exceptions under GDPR applies. See point 3 below discussing the consent and "legitimate interest" approaches.

2	Inform EEA residents about the use of their data	The company's privacy policy should both accurately and fully reflect its practices and address the wide array of requirements and disclosures mandated by GDPR. Some GDPR requirements that may be less-familiar to U.S. operators include: • A required statement of the purpose for which personal data is collected and processed. • The legal basis for processing data. See Point 3 below on consent. • The categories of third parties with whom the data is shared. • A disclosure of how long the data will be stored. • A statement of the EAA data subject's rights. For example, the right (i) to request access to, correction, or erasure of the data, (ii) the right to object or restrict the processing, and (iii) the right to data portability. • Where consent is given, the right to withdraw the consent at any time without affecting the lawfulness of any processing made prior to the withdrawal. • The right to lodge complaints with the relevant data protection authorities.
3	Consent or "Legitimate Interest" as basis for additional uses of data	The use of personal information to engage in targeted marketing or certain other activities that invoke the application of GDPR typically will require either the consent of the consumer, or the ability of the operator to demonstrate its "legitimate interest" in the marketing activity is not overridden by the consumer's fundamental rights and freedoms requiring protection of personal data. The consent and the legitimate interest requirement are discussed separately, followed by a brief summary of the additional requirements for e-mail marketing. **Consent**: Consent for marketing or sharing must be freely given, specific, informed, and unambiguous. Where required, consent has to be (a) voluntary (it *cannot* be a condition of using a site or service), (b) specific as to each type of use of data beyond the immediate transaction, (c) written in plain language an ordinary consumer can understand, and (d) unambiguously communicated, and not assumed based on merely continuing to use a site or otherwise not taking an affirmative step to opt out. Pre-checked boxes specifically are rejected. **Legitimate Interest**. The scope of the "legitimate interest" basis is not fully clear as of this writing but may be illuminated by future guidance from the European authorities. A portion of the GDPR refers to "direct marketing" as possibly fitting within an operator's legitimate interests. However, relying on that theory requires the operator to conduct a formal internal "legitimate interests assessment," including a determination of why the processing of personal data is necessary for the marketing activity, what benefits the company and its customers stand to gain, what potential harms the consumers face, whether the particular uses are consistent with the consumers' reasonable expectations, whether any less-intrusive options were available, and other

		factors. The main advantage of relying on "legitimate interest" is the ability to avoid obtaining affirmative consent, and the consumers' corresponding ability to revoke consent (though the consumer can lodge an objection to the data uses with the data protection authorities at any time thereby triggering an opportunity for the operator to seek to defend its practices). The main disadvantage is the uncertainty at this time about the scope of what will be accepted as a "legitimate purpose" for marketing purposes. **Email Marketing**. U.S. companies that wish to send marketing communication to consumers in the EEA **by email** also should consider the specific requirements for unsolicited electronic communications imposed by the EU E-Privacy Directive (which is currently under review and likely to be replaced by a new E-Privacy Regulation within the next year). The Directive prescribes that marketing emails may only be sent to individuals who have given their prior consent and does not recognize legitimate interest as a viable alternative. Consent is not necessary where the marketing is directed to existing customers and relates to products or services that are similar to those previously sold to the consumer as long as the consumer is sufficiently given the opportunity to object to the use of their email address.
4	Adopt Internal Data Security Measures	Implement and maintain appropriate technical and organizational measures to ensure an appropriate level of security for personal data.

5	Execute data processing agreements with third party service providers (sub-processors)	Data processing agreements with cloud service providers and other third party service providers which process personal data of EEA residents on the operator's behalf must include a number of provisions. A partial list of some types of mandatory provisions a U.S.-based company might not expect includes the following (along with many other requirements):
		
		• subject-matter, duration, nature, and purpose of the processing.
		• type of personal data and categories of data subjects.
		• operator's obligations and rights vis-à-vis the service provider.
		• the service provider's obligation to:
		  ◦ process personal data only on the operator's documented instructions.
		  ◦ ensure that all personnel authorized to process personal data have committed to confidentiality.
		  ◦ implement appropriate technical and organisational measures to ensure data security.
		  ◦ assist the operator in responding to requests from EEA residents and fulfilling its data compliance obligations to such individuals.

		• delete or return all personal data upon termination of the services. • submit to an audit of its data processing procedures.
6	Respond to individual requests by data subjects regarding the processing of their data	Implement appropriate procedures for responding to individual requests from EEA residents regarding their personal data rights, which may include: • request to be informed about and to access their personal data that the operator is processing (right of access). • request to rectify inaccurate parts of their personal data (right to rectification). • request to erase their personal data where the operator is not or no longer allowed to process such data (right to erasure). • request to restrict the processing of their data (*e.g.*, in cases where the accuracy of the data is disputed) (right to restriction of processing).
7	Notify DPAs of data breaches	Implement appropriate procedures for notifying the relevant data protection authorities of a data breach concerning personal data of EEA residents.
8	Maintain a record of processing activities	If a company has more than 250 employees, it must maintain a record of processing activities which must be made available to the relevant data protection authorities upon request.
9	Delete personal data	Delete all personal data of persons residing in the EEA where such data is no longer necessary for fulfilling the purpose for which the data were collected, unless retention is required by applicable law.
10	Designate a representative in the EEA	Designate in writing a representative in the EEA to be available to respond to requests by the EU data protection authorities or persons in the EEA on issues relating to the processing of personal data under GDPR.

The above is just a general overview of some of the requirements under GDPR for a typical U.S.-based website operator seeking to engage in e-commerce and/or online marketing. The focus is on sales and marketing-related issues. There are numerous other compliance requirements, including for internal data security, contracts with vendors, etc. Individual requirements will vary based on a company's particular operations. Given the complexity of the issues under GDPR, the current unclear status of the interpretations of the 99 articles that make up the GDPR, and the delicate balancing of pros and cons for relying on various grounds using data, U.S.-based companies should consult with legal counsel familiar with GDPR issues to help guide their decisions on how to proceed.

Authors

This GT Alert was prepared by **Alan N. Sutin, Dr. Viola Bensinger, Ed Chansky, Francoise Gilbert** and **Carsten Kociok**. If you would like assistance in reviewing your current website privacy practices for possible compliance with GDPR, contact:

- Alan N. Sutin | +1 212.801.9286 | sutina@gtlaw.com
- Dr. Viola Bensinger | +49 (0) 30.700.171.150 | viola.bensinger@gtlaw.com
- Ed Chansky | +1 702.599.8016 | chanskye@gtlaw.com
- Francoise Gilbert | +1 650.804.1235 | gilbertf@gtlaw.com
- Carsten Kociok | +49 (0) 30.700.171.119 | carsten.kociok@gtlaw.com
- Or your Greenberg Traurig attorney