The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 3, No.25 December 20, 2017

GDPR

Five Months Until GDPR Enforcement: Addressing Tricky Questions and Answers

By Scott Pink, O'Melveny & Myers, Hayley Ichilcik, O'Melveny & Myers, Mallory Jensen, O'Melveny & Myers

With five months to go before the E.U.'s General Data Protection Regulation (GDPR) takes legal effect, most companies have, by and large, determined whether the GDPR will apply to them and, if it will, have begun to take steps to comply. (And for companies that have not yet made this determination, now would be a good time to start thinking about it.)

The question of whether a company is subject to the GDPR is thorny enough. But once a company has determined it falls within its boundaries, even more difficult questions begin to arise as it grapples with the complicated process of applying the many provisions of the GDPR to existing and past data privacy practices. In preparing for compliance with the GDPR, a number of common questions arise from organizations across a variety of industries. The following Q&A provides a glance at some of the issues that companies are grappling with in understanding the GDPR's reach.

See also "One Year Until GDPR Enforcement: Five Steps Companies Should Take Now" (May 31, 2017).

1. Do GDPR requirements apply to existing data collections and past transfers of data?

Yes, the GDPR applies to ongoing processing and maintenance of data, even if the data was collected in the past. Both the GDPR and guidance from some E.U. Member States' Data Protection Authorities (DPA) support this view. Companies must be in full compliance with the GDPR as of May 25, 2018. Beginning on that date, any future processing of data, regardless of when it was obtained, will need to comply with the GDPR. This might require changes in how existing data is handled, or that new consents be obtained for the handling of such data.

When the basis for processing is consent from the data subject, and that consent is based on the prior Data Protection Directive 95/46/EC, the GDPR does not require obtaining consent from the data subject again **provided that** "the manner in which consent has been given is in line with the conditions of" the GDPR. Following this approach, the British Information Commissioner's Office's draft guidance on consent under the GDPR notes that "if existing DPA consents don't meet the GDPR's high standards or are poorly documented, [companies] will need to seek fresh GDPR-compliant consent, identify a different lawful basis for [their data] processing (and ensure continued processing is fair), or stop the processing." But the Italian DPA has explained that the consent obtained before the date of effectiveness of the GDPR continues to constitute a valid form of consent if it has been collected in such a way as to be "explicit" (when it comes to collecting sensitive data and decisions based on automated processing), "free, specific, informed" and "manifested through unambiguous declaration or action" (if referred to ordinary data).

See also "Getting to Know the DPO and Adapting Corporate Structure to Comply With the GDPR (Part One of Two)" (Jan. 25, 2017); Part Two (Feb. 8, 2017).

2. What manifestations of consent are sufficient? Specifically, is there any guidance on what would be sufficient to constitute "clear affirmative actions" showing "freely given, specific, informed, unambiguous indication"?

The GDPR provides some guidance on the issue of what constitutes adequate consent. And so has the Article 29 Working Party (which in the past provided expert advice to E.U. states on data protection, and which the GDPR replaces with the European Data Protection Board, with the addition of an independent secretariat). Although some of the guidance comes in negative form (i.e., indicating what does not qualify as consent) it can still be useful to companies in demonstrating what they must do to obtain valid consent.

- "Clear, affirmative actions": The GDPR provides that such actions may include "a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information-society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data." By contrast, "[s]ilence, pre-ticked boxes, or inactivity" do not constitute adequate consent.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 3, No.25 December 20, 2017

- "Freely given" consent: Consent is not freely given if the data subject has no genuine and free choice or is unable to refuse or withdraw consent without some detriment, or if there is a clear imbalance between the data subject and the controller. In the employment context, in particular, the inherent imbalance of power between employer and employee means that some may argue that consent is not freely given and is therefore invalid. In addition, the GDPR indicates that consent is presumed to not be freely given if consumers are not allowed to give separate consents for different data processing operations when appropriate. In other words, "bundled" consents are likely inadequate and unenforceable.
- "Specific" consent: Broad consent forms that purport to give a company the consumer's permission to process data for a wide variety of purposes based on one single consent are unlikely to be enforceable under the GDPR. Instead, "[c] onsent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them."
- "Informed" consent: The GDPR also prescribes what makes a consumer's decision to consent appropriately "informed." Specifically, the consumer must be aware of at least (1) the data controller's identity and (2) the purpose(s) of the processing of the consumer's personal data.

Given the more onerous nature of consent under the GDPR, it may be more attractive for companies to rely upon another legal basis (to the extent possible) in relation to obtaining personal data from employees (although in Germany it has been accepted that consent can be relied upon in the employer/employee context).

3. Can an entity condition provision of the company's services on individuals providing consent for the company's desired data uses?

As described above, the GDPR specifically provides that companies may not condition providing their services to individuals based on consent to data processing, if that processing is not necessary to the contract or provision of services. It may be appropriate for a company to require consent to data processing before providing the contracted-for services, if the data is necessary for the company to perform the services. But if, on the other hand, the company cannot demonstrate that the data processing is necessary for it to provide services under the contract, it cannot require consent for data processing before providing the services.

The small sample of questions and answers provided in this article shows the complex territory that companies are entering as they work to become compliant with the GDPR. Undoubtedly, in the next six months before the GDPR enters into force, as well as after, even more questions and complications will arise. However, by working out how to respond to these questions now, companies will position themselves well for the GDPR's enforcement after May 2018 and reduce the risk of fines or questions of non-compliance.

See also "A Discussion With Ireland's Data Protection Commissioner Helen Dixon About GDPR Compliance Strategies (Part One of Two)" (Mar. 22, 2017); Part Two (Apr. 5, 2017).

4. In what types of circumstances does the GDPR (including the provisions for significant fines in enforcement actions) apply to non-European parent companies in addition to the subsidiaries that operate in Europe?

The answer to this question depends on the data collection and processing activities of the parent company. The GDPR by its terms applies both to processors or controllers based in the E.U. and to the processing of data by controllers or processors not based in the E.U. where the processing activities are related to (a) the offering of goods and services to data subjects in the E.U. or (b) the monitoring of their behavior to the extent it occurs in the E.U. So, any entity within the corporate organization that fits within these definitions is required to comply with the GDPR.

Furthermore, the GDPR applies to any processing of personal data in the context of a controller or a processor established in the E.U., regardless of whether the processing takes place in the E.U. or not. If a subsidiary is established in the E.U. and the parent itself processes personal data "in the context" of that subsidiary's activities, for example, by providing human resources support to the subsidiary, then the GDPR could apply to the parent's processing activities.

A U.S. entity also could be subject to the GDPR by virtue of the transfer of E.U. individual's personal data from an E.U. subsidiary to the U.S. entity. Such transfer may be subject to binding corporate rules approved by the competent supervising authority or based on the Privacy Shield. Under the GDPR, the required elements of binding corporate rules include, among other things, the application of the GDPR principles to the processing of the data transferred.

Moreover, the potential application of administrative fines for GDPR violations may be broader than the application of the GDPR requirements themselves. GDPR's provisions regarding fines use the term "undertaking" in referring to businesses. The term 'undertaking' should be understood in accordance with the Treaty on the Functioning of the European Union (TFEU). The law regarding Articles 101 and 102 of TFEU indicates that where one company exercises "control" over another company, they form a single economic entity and, hence, are part of the same "undertaking." The GDPR similarly states that a controlling undertaking is an undertaking that can exert a dominant influence over the other undertakings by virtue, of its ownership, or the power to have personal data protection rules implemented.

This includes situations in which a parent is a majority shareholder in a subsidiary. Since the parent is in the position to exercise control over that subsidiary, there is a rebuttable presumption that the parent does exercise such control. Where the parent is a minority shareholder, there is no presumption of control, and a range of factors will be taken into account to assess whether they have control, including: the size of the parent's shareholding; representation on the board of directors of the subsidiary; the ability to influence the commercial policy of the subsidiary; and evidence of efforts to do so.

5. Can an international company manage GDPR financial risks through corporate layering or structuring to protect non-E.U. operations from being counted in total gross revenues at risk?

The principles discussed above make it difficult to shield a controlling entity like a parent company from the potential for GDPR administrative fines, even if that entity is not actually processing or directing the processing of personal data. This is because: (a) the parent of such subsidiary likely will be deemed a controlling undertaking, with resulting GDPR responsibility, by virtue of its ownership interests in the subsidiary, and (b) the parent also could liable for its own activities that affect E.U. data subjects. The administrative fines in the case of an "undertaking" could be as much as 4 percent of annual worldwide turnover, or €20 million (whichever is higher). If the parent is considered part of an undertaking based on the principles above, the fines could be based on the annual worldwide revenue of the parent and its subsidiaries.

However, there may be ways to structure organizations where key assets are held in related entities that do not control the E.U. operations and so may not fall within the definition of an "undertaking" for GDPR responsibility purposes. Companies also should consider whether the liability protections afforded to corporations could potentially be used as a shield to liability, particularly if the parent entity has no assets or operations directly in the E.U. For the avoidance of doubt, however, if a parent company that is based outside the E.U. receives the personal data of E.U. individuals and processes such data in relation to (a) the offering of goods and services of data subjects in the E.U., or (b) the monitoring of their behavior to the extent it occurs in the E.U., in each case such parent company may be subject to the GDPR regardless of the corporate structure in place.

6. Can companies use pre-existing data breach response plans to comply with the GDPR, or is something different required?

The answer to this question depends, of course, on what kind of incident response plan the company had before the GDPR, and whether it was tied to the requirements of any particular jurisdiction. The GDPR requires any company that experiences a data breach to publicly acknowledge the breach and notify the local DPA in the member states where the people affected by that breach reside. Notification to the DPAs must happen within 72 hours of identification or confirmation of the breach. The company must be able to tell the DPAs what data was breached, how many records were taken and provide a member state-specific report around the infringement. This requirement essentially means that the company must be able to understand who accessed the data, what they did with the data, and when, all within a very short time frame. If the company's current data breach response plan does not provide the tools to make these determinations quickly, it should revisit the plan and make adjustments accordingly.

See also CSLR's three-part guide to developing and implementing a successful cyber incident response plan: "From Data Mapping to Evaluation" (Apr. 27, 2016); "Seven Key Components" (May 11, 2016); and "Does Your Plan Work?" (May 25, 2016); and "Checklist for an Effective Incident Response Plan" (Jul. 20, 2016).

7. Can a U.S. company be liable under GDPR when another entity is the one who provided the E.U. individuals' data, as distinct from the U.S. company obtaining that information directly

In certain circumstances, it can be liable. The GDPR applies to both controllers (i.e., those responsible for determining the purposes and means of the processing of personal data) and data processors – organizations who may be engaged by a controller to process personal data on their behalf (e.g., as an agent or supplier).

Under GDPR, processors will be required to comply with a number of specific obligations, including to maintain adequate documentation, implement appropriate security standards, complete routine data protection impact assessments, appoint a data protection officer, comply with international data transfer requirements and cooperate with national supervisory authorities.

These obligations are in addition to the requirement for controllers to ensure that when appointing a processor, a written data-processing agreement is put in place meeting the requirements of GDPR. Processors will be directly liable to sanctions if they fail to meet these criteria and may also face private claims by individuals for compensation.

8. What contractual and diligence steps should a U.S. company take before receiving personal data of E.U. individuals from another entity? For example, what certifications or representations should the company seek about the consent the entity obtained that may apply to the U.S. company's activities?

The U.S. company will want to confirm that the other entity has complied with GDPR requirements in connection with the processing of E.U. personal data. This might include obtaining copies of any consent forms used to collect such data and understanding how and why information is collected and how it relates to the purposes for which it was collected. Companies should consider developing due diligence questionnaires or checklists to make sure they get sufficient comfort about GDPR compliance before proceeding.

U.S. companies will also want contractual protections in their agreements with other entities, including warranties of GDPR compliance and robust indemnification against claims relating to violation of GDPR requirements. U.S. companies receiving E.U. personal data should seek to ensure that such transfer is GDPR compliant and may consider requiring their vendors to provide such certifications or code of conduct to evidence that the transfer of such data is GDPR compliance.

Scott Pink, formerly general counsel for media and publishing company Prima Communications, advises technology, media, entertainment and a variety of consumer product and franchise companies on issues of intellectual property counseling; social media law; cybersecurity and privacy; and advertising, marketing, and promotions law.

Hayley Ichilcik specializes in multijurisdictional corporate investigations, white collar criminal defense, complex civil litigation, and international arbitration. She is in the London office and is a Solicitor-Advocate with full rights of audience before the English courts.

Mallory Jensen is litigator specializing in complex civil disputes, regulatory matters, internal investigations, antitrust litigation, data security and privacy matters, and intellectual property disputes.