The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 12 May 16, 2018

GDPR

Countdown to GDPR Enforcement: Final Steps and Looking Ahead

By Scott Pink, Mallory Jensen, Amanda Bradley
O'Melveny & Myers

In the short time before the GDPR goes into effect, and in the first stretch of its life as the law of the land across the E.U., what are the last-minute steps that companies should be taking to prepare themselves for this sea change in privacy rules? Representatives from E.U. member states' Data Protection Authorities (Authorities), which will enforce the GDPR, have emphasized that there will be no "grace period" for companies at the beginning of the GDPR's effective period – after all, companies have already had a year in which to prepare themselves. At the same time, the Authorities have also taken care to emphasize that those companies that have made serious efforts to come into compliance will not be the main targets of scrutiny or enforcement actions. And in the event that a member state's Authority does think that a company is not in compliance, they will likely not be fined immediately, but rather will be subject to various preliminary sanctions, beginning with a warning.

This article assumes that by now, if a company is subject to the GDPR, it is both aware of that and has taken basic steps to comply with the regulation, such as data mapping, updating privacy policy and consent procedures, appointing a Data Protection Officer (DPO) if necessary, implementing procedures for handling data subject access requests, and confirming the company's ability to report any data breaches to the relevant E.U. authorities within 72 hours. To the extent some of these important initial steps have not been taken, they should remain a company's first priority. But if those steps are complete, what are some other important steps to consider? And once the company is generally in compliance with GDPR, is there anything more to do to ensure that it will not be in regulators' crosshairs as they begin their examinations?

As this article explains, there are likely some additional areas of GDPR compliance that companies have not yet thought to address, but that could make an important difference in protecting users' or customers' privacy.

Moreover, companies must remain vigilant and continue improving their privacy procedures after the GDPR takes effect: it has ongoing compliance obligations that will keep the company occupied for the foreseeable future, as they become just another part of doing business. Companies also will need to be mindful of different member states' specific approaches to GDPR, articulated in implementing legislation and regulations set out by their respective Authorities. Only four member states have passed such legislation, so there are many developments still to come in this regard.

See also the CSLR's two-part interview with the Irish Data Commissioner: "Supervising Facebook" (April. 25, 2018); and "GDPR Enforcement Priorities" (May 2, 2018) and "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).

Importance of Data Processing Agreements and Addendums

First, companies should put in place data processing agreements (DPAs) to govern the processing of personal data by a processor on behalf of a controller. A DPA governs the roles and responsibilities of the controller and the processor, and may also address the allocation of liability between them. It is important to have a DPA in place so that the relationship between, and respective roles of, the parties are clearly established.

Details to Include in the DPA

As a threshold matter, DPAs should establish such details as:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data being processed;
- the categories of data subject to the processing; and
- the obligations and rights of the controller.

Importantly, DPAs are required to address certain obligations of the processor as set forth in Article 28, including: an obligation to act in accordance with the controller's written instructions (unless otherwise required by law), an obligation to maintain confidentiality of personal data that it processes, an obligation to assist the controller in meeting its obligations related to security, breach response, conducting data

protection impact assessments and the like.
Controllers may also seek to include an indemnity for the processor's handling of personal data, and an obligation of the processor to return or destroy any personal data at the end of the relationship or upon other triggers. DPAs typically include, by their terms or incorporated as an exhibit, a version of the Standard Contractual Clauses which were established by the European Commission pursuant to the EU Data Protection Directive 95/46/EC. When used in connection with a DPA, these Standard Contractual Clauses should be updated to comply with the GDPR, as so far no standard contractual clauses have been made available by the relevant supervisory authorities under GDPR.

When to Use a Data Processing Addendum

In cases where companies have in place existing agreements with vendors or other third parties that involve the processing of personal data, it may be most expedient to put in place a Data Processing Addendum. A Data Processing Addendum simply amends the existing agreement to provide that the processing of personal data shall be performed in compliance with certain terms, such as those required by the GDPR (which should also be the same terms that one would include in a DPA).

Putting in place a DPA or Data Processing Addendum is not just a good practice for establishing a mutual understanding regarding these matters - a written contract for processing is an express requirement of the GDPR (Article 28). As such, companies would be wise to put such contracts in place as soon as possible. For large companies with hundreds of contracts, this will clearly be a substantial undertaking.

Companies that do not have data processing arrangements in place, then, are advised to create a risk-based plan for establishing compliance, prioritizing those contracts or vendor relationships where data processing is a key component or where the largest amounts of personal data are processed. Companies should also thoroughly document all efforts to achieve compliance in a timely manner, particularly where such efforts may be met with resistance from counterparties.

Consents for Email Marketing

GDPR has a direct impact on marketing practices, including email marketing. While many of the underlying principles of the GDPR are consistent with the prior E.U. privacy framework as it relates to marketing (such as the E.U. Privacy Directive requirement that recipients must opt in to most email marketing), most companies must (if they have not done so already) take action to bring their marketing efforts into compliance with the more stringent requirements imposed by the GDPR. In addition, the E.U. Privacy Directive is expected to be replaced with the new ePrivacy Regulation after the GDPR is effective. In the meantime, E.U. Privacy Directive rules are expected to be applied using the GDPR definition of consent.

What Is Adequate Consent?

As discussed in prior articles, one of the most significant ways the GDPR impacts marketing practices is through its guidance on what constitutes adequate consent. While the GDPR is consistent with the E.U. Directive requirements that consent be "freely given," "specific," and "informed," the GDPR is clear that consent must also be "unambiguous" and signified by a "clear affirmative action." Significantly, this means that pre-ticked opt-in boxes – or any form of consent similarly based on the data subject's inaction or inattention, or the default settings of the consent request mechanism - do not constitute adequate consent. The data subject must take an affirmative action (such as ticking an empty box) to opt in to receive marketing emails, in order for the consent to be valid.

Consents to email marketing must also be separate from consents given for other purposes. If, for example, certain processing activities are necessary for the provision of a service, the consent to processing in connection with that service must be separate from - and not bundled with - the consent to marketing. The data subject must have the freedom of choice to accept the necessary processing but decline to opt in to processing for marketing purposes. Accordingly, requests to consent to email marketing that are provided in the company's first interaction with the data subject must appear separately (e.g., with a separate ticked box) from any other consents being gathered in the same interaction.

See "One Year Until GDPR Enforcement: Five Steps Companies Should Take Now" (May 31, 2017); "Five Months Until GDPR Enforcement: Addressing Tricky Questions and Answers" (Dec. 20, 2017).

Data-Subject Rights

The GDPR also empowers data subjects with further rights to control the manner in which their data is processed. Importantly, in the marketing context, data subjects have the right to object to direct marketing, and the right to withdraw

any consent previously provided. The right to object requires companies to stop processing upon receipt of an objection. Companies must also provide data subjects with a clear means of withdrawing a consent previously given, which must be as easy to do as it was to provide the consent in the first place. Including an "Unsubscribe" link in each marketing email is likely sufficient.

When to Seek New Consent

Companies that previously obtained consents to email marketing may rely on those consents if they were obtained in a manner consistent with what the GDPR now requires. If a consent was not obtained in a GDPR-compliant manner – if, for example, the consent to receive marketing emails was bundled with the consent to processing for services and/or was presented to the data subject in a pre-ticked box – the prior consent is invalid and new consents must be obtained.

Companies should seek new consents now and notify customers that if they do not provide their consent to email marketing, they will no longer receive such communications from the company. In connection with obtaining new consents, and any other time a company relies on consent as the basis for data processing, it should record and evidence the details of that consent (who provided it, when and how they did so, and what information they received at the time).

Companies may be reluctant to make good on the promise that no further marketing email communications will be sent to recipients who do not provide GDPR-compliant consents – but they should be aware that there may be significant consequences for not doing so. Failing to comply with GDPR requirements, including the requirements described above, could result in fines of up to €20 million or 4 percent of total worldwide annual turnover, whichever is higher. And even if consent to email marketing may seem like a relatively minor detail, it is important to keep in mind that failure to meet the GDPR's requirements in one regard is likely to draw regulators' attention to potential failings in other areas.

Ongoing Data Privacy Obligations

Finally, it is critical to understand that even if a company has managed to address all possible updates needed for GDPR readiness, the necessary work on the GDPR has only begun. The GDPR imposes a variety of privacy and data-security obligations that will continue to require ongoing attention. This section includes a non-exhaustive review of some of these obligations.

Process for Updating Policies/Consents

Transparency is a key element of GDPR, which means that ensuring your privacy policies, notices and consents be revised to be compliance with the GDPR requirements. The policies, notices and consent need to be continually monitored and updated as new processes and practices are implemented to make sure they are current and up-to-date.

Article 30 Record of Processing

Companies should already have created a database or document in which they can record all of their processing activities, as required by Article 30 of the GDPR. This record must be maintained and updated indefinitely so that the company can provide it to regulators if asked. The record of processing must include:

- contact information for the company, the DPO, joint controllers and any E.U. representative;
- the purposes of the data processing;
- the categories of individuals whose data is processed and of the data processed;
- information about countries to which personal data is transferred and about safeguards in place for transfers;
- data retention schedules; and
- a general description of the company's data security measures.

Since this is a living document, companies must constantly make sure that it reflects any changes to the type of data being processed and the purpose for the processing.

Data Security Requirements

The GDPR also requires that companies "implement appropriate technical and organizational measures." What is "appropriate" is measured not only by the level of risk involved in the company's process, but also by what is standard in the company's industry and in business generally – and that will undoubtedly change rapidly over time as the state of the art in cybersecurity protections advances. As a result, while an appropriate data security program should be implemented now (prior to the GDPR's effective date), it is essential for companies to stay up-to-date with what is the best suite of data security measures to protect the personal data that the company processes and stores. For example, if a significant improvement in encryption technology is developed,

companies will need to consider adopting it, because the older technology may no longer be sufficient.

See also "Using Technology to Comply With the GDPR" (Feb. 14, 2018).

Data Protection by Design and Default

The GDPR encourages companies to adopt a philosophy in which data protection and privacy are designed into their products and user experiences from the beginning, not just built on top of pre-existing products and processes as an afterthought. Taking this privacy-first approach allows companies to identify potential privacy issues early on, and address them or design around them from the start; too often, companies have had to fix design features that create privacy issues after those features have already been built into a product or system. This makes the fix for such issues much more complicated and costly. By accounting for privacy from the start, companies are also more likely to actually be compliant with the GDPR and other privacy laws, because privacy considerations will have been thoughtfully addressed at all stages of design, making for a more complete solution. This approach requires a strong commitment to privacy training and infrastructure throughout an entire company, not just in the legal or compliance departments.

Data Protection Impact Assessments

The GDPR institutionalizes the increasingly common practice of conducting data protection impact assessments (DPIAs) when a company is building a new product or service, or otherwise changing or updating its data processing, to assess how those changes will affect the company's use of personal data. The GDPR requires that such assessments be made whenever the company is going to conduct processing that "is likely to result in a high risk to the rights and freedoms of natural persons," in particular when the company is going to engage in "systematic and extensive" automatic profiling of people via their personal data, when it will be processing data in the special categories (such as gender, sexual orientation, religion, criminal record, etc.), and when the company is engaging in large-scale, systematic monitoring of a public space. Consistently producing DPIAs, even in contexts where the processing may not fall in one of the three scenarios where a DPIA is absolutely required, is an important way for companies to demonstrate GDPR compliance.

See also "Uber Settlement Highlights Benefits of a Privacy Impact Assessment" (Aug. 23, 2017).

Manage Vendors

It is important for companies to carefully monitor any third parties that may touch personal data collected by the principal company. Under the GDPR, companies that farm their processing or storage of personal data out to other companies, must make sure that those other companies are also following GDPR-compliant procedures. This means that not only must companies evaluate their vendors now, going into the GDPR enforcement period, they must also, going forward, pay attention to data privacy and security practices of existing and new vendors, and impose tighter controls to ensure that these outside companies are taking appropriate measures to protect the data (one important step to accomplishing this is by entering into DPAs, as discussed above). Companies will also want to scrutinize both their own practices for transferring data to third parties, and the third parties' practices in that regard, to determine whether necessary safeguards are in place.

See CSLR's two-part series on vendor risk management "Nine Due Diligence Questions" (May 25, 2016), and "14 Key Contract Terms" (Jun. 8, 2016).

Respond to Individual Rights Requests

The GDPR also implements a bill of rights for individuals whose personal data is handled by companies, giving them, for example, a right to have their personal data corrected or deleted and requiring that companies honor requests for such correction or deletion. Companies should have already been thinking through this obligation and creating a process to handle such requests, but it will be an ongoing commitment both to respond to such requests and to engage in creative thinking and problem-solving surrounding such requests, as different types of data and different types of processing are introduced and requests for correction, deletion, portability of data, and so on will need to be handled in different ways.

The privacy landscape will look very different after the GDPR goes into force. It will take time for regulators and companies alike to navigate that new landscape, despite the long run-up to effective date of enforcement. But companies that enter the new GDPR world having taken a measured, comprehensive approach to ongoing compliance will be well-positioned to meet the challenges of the GDPR regime.

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.

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

Amanda Bradley is a corporate associate in O'Melveny's San Francisco office