Better Late than Never

Considerations for GDPR Compliance

By Phil Busman
and Colton Driver

The deadline for GDPR compliance has passed, but for many clients, there is still time.

Europe's new General Data Protection Regulation (GDPR) has been a major buzzword this year. And as is the case with many buzzwords, a lot of clients and practitioners have likely tuned it out, thinking that it would never apply to them. However, most clients have probably never had to consider data protection issues on this level before, and the GDPR will affect a lot of people who never imagined being subject to this type of regulation. For that reason, writing it off is probably a mistake.

The good news is that even though the May 25, 2018, deadline has come and gone, it is not too late for your clients to get up to speed. And your clients with GDPR-related concerns can rest assured that they are not alone. Up to 80 percent of companies in the United States, United Kingdom, and European Union required to comply with the EU's new GDPR are not yet ready. *See* Edward Gately, *80 Percent of Companies Still Not GDPR Compliant*, Channel Partners News (July 13, 2018, 13:08); Sue Reisinger, *85 Percent of Companies Not Fully Ready for the GDPR, Survey Says*, Legal Tech News (LAW.COM) (May 21, 2018, 16:41). Many of those companies have likely not even started the compliance process. More importantly, the general consensus seems to be that EU regulatory authorities tasked with GDPR enforcement are not ready yet, either. *See* Douglas Busvine *et al.*, *European Regulators: We're Not Ready for New Privacy Law*, Reuters (May 8, 2018, 6:34). For those among us in the same boat, although the clock is ticking, there is still time to develop a basic understanding of the GDPR framework that is sufficient to advise clients on the general steps necessary to get them moving in the right direction.

Having said that, compliance is a *process*. And processes take time to consider, create, change, or implement. So if you find yourself advising a client about the GDPR, time is of the essence. This article is written with an eye toward prioritizing GDPR compliance issues that could potentially help your clients make up the most ground in the shortest amount of time. We highlight key takeaways from the GDPR to foster conversation with your clients about some of the most important items to think about up front until both you and your cli-

■ Phil Busman is a partner in Nelson Mullins Riley & Scarborough LLP's Washington, D.C., office focusing on complex litigation, including mass and consolidated actions. Colton Driver is an associate in the firm's Columbia, South Carolina, office, where he focuses his practice on electronic discovery and a variety of related issues with the Encompass e-discovery group.

ents are far enough ahead of the curve to focus on some of the finer details.

Does It Apply to Your Client?

There is a fairly common misconception that GDPR protections are based on citizenship. They are not.

GDPR Article 3: A Data Subject's Location

GDPR protections are based on a data subject's *location* in the EU. Article 3(2). Moreover, the GDPR protects only *personal* data of natural persons. So, to the extent that purely business-to-business information is in question, the GDPR does not apply.

While the protections of the GDPR are limited to a data subject located in the EU, the obligations that it imposes on companies reach far beyond the EU's borders. So how do you determine whether the GDPR applies to your client? The answer is found in Article 3(2), which states, "This Regulation applies to the processing of personal data of data subjects who are in the Union." The main takeaway from Article 3 is that for your clients located in the EU, the GDPR applies no matter where they do their data processing. For clients not based in the EU, the GDPR applies *only* when a business offers goods or services to EU residents (no payment is required), monitors EU data subjects' behavior taking place within the EU, or processes data in a non-EU country where member state law applies vis-à-vis public international law.

If you are advising a client with no resources or facilities within EU borders that does not offer goods and services to residents of the EU *and* neither monitors subject behavior nor collects data associated with subject behavior (*e.g.,* for marketing or advertising purposes), the GDPR does not apply. Thus, a brick-and-mortar store in the United States that does not ship to the EU or offer business to the EU does not have to comply with the GDPR even if a citizen of the EU makes a purchase at the store. It is nevertheless a good idea to get those clients moving in the general direction of GDPR compliance because American states have already begun tightening their data protection rules to mirror GDPR standards. This June, California passed some of the strictest data privacy legislation in the country, which is set to go into effect in January of 2020. *See* Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. Times (June 28, 2018). This was right on the heels of action taken in Vermont, where legislators passed a law in May regulating so-called data brokers.

A good first step for most clients (once you decide that the GDPR applies to them), would be for them to conduct a data audit to really get a handle on what types of data they are collecting and where the data is being stored. Knowing that information will allow a much more beneficial conversation as you work your way through the remainder of the GDPR.

What Is Your Client?

While the article-by-article distinctions are beyond the scope of this writing, you need to determine what your client's role is, as defined by the GDPR.

GDPR Article 4: Controller or Processor?

Your client might be a *controller*, a *processor*, or both. Article 4 defines each, as well as a number of other terms. A controller "determines the purposes and means of the processing," while a processor "processes personal data on behalf of a controller." *Processing* is defined as "any operation or set of operations which is performed on personal data… such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use… erasure or destruction." So while "processing" sounds active, if your client is even looking at personal data, that client may be deemed to be processing it.

Bases for Processing Data: Is Consent the Best?

There is another apparently widespread misconception about the lawful bases for processing data under the GDPR: namely, that consent is required in all cases.

GDPR Article 6: What Role Does Consent Play in Processing?

While consent of a data subject is the first lawful basis listed in GDPR Article 6, consent alone may prove a shaky foundation for processing data because a data subject can withdraw consent at any time. Although withdrawal of consent does not invalidate the legitimacy of data processing done to that point, it severely limits the extent to which a company can continue using the data previously collected with consent. Thus, encouraging clients to rethink how they obtain and record consent post-GDPR is crucial. But so is encouraging them to have a fallback basis for processing data.

In the context of litigation, relying on consent by itself is further problematic because there is no guarantee that your opponent will agree to produce any of the data that you need. Moreover, consent must be expressly tied to each purpose for which the data is used. Thus, even if a particular data subject were to provide consent for a business purpose, serious doubt remains as to whether such consent can later be construed to extend to production of the same data to a third party in litigation. While the GDPR makes provision for various exceptions in the context of litigation, this is uncharted territory, and the contours of various legal exceptions have not yet been defined. These are the types of questions that are being asked, and as the GDPR is enforced, it remains to be seen how EU and American courts will navigate these issues.

A good first step for most clients (once you decide that the GDPR applies to them), would be for them to conduct a data audit to really get a handle on what types of data they are collecting and where the data is being stored.

While consent is the first of six lawful bases for processing data, unless your client is based in the EU and you have sufficient knowledge of individual member state laws to advise them on those laws, your client may have less than six options. That is because the bases contained in Arti-

cles 6(1)(c) ("necessary for compliance with a legal obligation") and 6(1)(e) ("necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller") are limited in scope by Articles 6(3)(a), 6(3)(b), and Recital 45 to respective obligations or interests arising from EU law or member state law. So if a legal obligation stems from U.S. law, for instance, there is considerable doubt that it would be treated in the same manner as one arising under EU law.

Consent presents a unique set of challenges for employers with EU data subjects as employees.

That effectively leaves your client with four potential bases to rely on for lawful data processing: consent, contract, protection of the vital interests of the data subject or another, or legitimate interests. One interesting note—"legitimate interests" is *not* a basis that the GDPR allows public authorities to use in the performance of their tasks as public authorities, perhaps out of concern for governmental abuse. And using that as the basis will come with a balancing test that weighs the identified legitimate interest against the interests of the data subject in question, among other things.

One particular area where this should be in focus for clients is the employment context. Consent presents a unique set of challenges for employers with EU data subjects as employees. Article 7 addresses the requirements for consent in greater detail, and Recitals 32, 33 (beyond the scope of this article), 42, and 43 touch on the unique requirements associated with consent in greater detail.

Article 7(4) stresses that consent must be freely given, which poses a unique conundrum when an employee does not want certain information shared but is required to consent to data collection or processing as a condition of employment. Given the power imbalance in such situations, there is a question whether the consent was "freely given," particularly in light of Recital 43, which stresses that "consent should not provide a valid legal ground for the processing of personal data… where there is a clear imbalance [of power] between the data subject and the controller."

This could also come into particular focus for some governmental data processing, of which the GDPR already appears skeptical, given its limitations to governmental authorities using the legitimate interest justification. Recital 32 requires that consent be given by a "clear, affirmative act," so your clients should consider making an actual "check" box or an "accept" button that has to be clicked if they currently rely on a pop-up to obtain consent in a website setting. The next important piece of the consent puzzle is that a controller must be able to *demonstrate* that a given data subject has consented as required by Recital 42—which makes consent tracking absolutely imperative. Thus, encourage your clients to really think through their bases for processing because they are perhaps the most core piece of GDPR compliance.

Access, Rectification, Erasure, and Transparency

On their respective faces, what Articles 12–17 ask of your clients is simple: 30 to 90 days to respond to requests for access, rectification, or erasure. Unfortunately, while these articles are simple in theory, they are complex to implement in practice from a logistical standpoint.

GDPR Article 12, 13, and 14: Efficient Notification, Tracking, and Data Subject Request Processing

Article 12 applies to any requests issued under Articles 15–22. While not all are discussed here, it is important to note the key role that Article 12 plays regardless of the type of request. Article 12(3) states:

> The controller shall provide information on access taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

The provision further provides that notification of any extension must be made to the requesting person within the initial month after the request.

The overarching point is that compliance with Article 12's mandate requires robust standard operating procedures and infrastructure to allow for the efficient tracking and processing of data subject requests. In this respect, access and erasure requests have something in common with security breach notifications under the GDPR, albeit with a far less daunting timeline (more on that later). For many clients, this will require tech-side initiatives that allow a client to locate any specific EU resident's data in any of its systems in a relatively short time. Moving forward, that could even involve implementing new policies regarding the fields where customer data is entered to reduce the number of potential places where this data could be stored. While this particular piece is not legal in nature per se, it is still something that lawyers need to ensure is on a client's radar.

From a last-minute compliance perspective, your controller clients' primary goals here are to work out a system that allows them to locate and isolate a particular data subject's information and to respond to any request within a month (ideally). Efficiency is important because of the breadth of requests that a data subject is allowed to make, but also because "[i]nformation provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 (discussed further below) *shall be provided free of charge*." Article 12(5) (emphasis added). Thus, your clients will need to account for these additional costs in their business planning, since as a general rule, they are not allowed to pass costs through to data subjects.

Rights

There are a number of rights that any GDPR-bound client's infrastructure must account for.

Right of Access (Article 15)

Article 15 essentially states that data subjects have a twofold right from any controller: (1) a right to *confirmation* of whether or not personal data concerning them is being processed, and (2) when that is answered in the affirmative, a right of *access* to the personal data (and a copy of it, under Arti-

cle 15(3)), as well as a number of pieces of information required under Articles 13 and 14, which are reiterated in Article 15.

Right to Rectification (Article 16)

Data subjects have the right, without undue delay (but in any case, within the same 1–3 month timeline laid out in Article 12), to have incorrect or incomplete data corrected. Clients will need to develop a system to identify and correct errors when informed about them by data subjects, while still making sure that their businesses run efficiently. Individual clients will need to tailor their system to their business; some may choose to update this data immediately, while perhaps another client may correct changes on a set schedule such as weekly or monthly.

Right to Erasure ("Right to Be Forgotten") (Article 17)

The right to erasure is one of the more legally controversial rights contained in the GDPR. Under Article 17, commonly referred to as the "right to be forgotten," data subjects have a right to force processors and controllers to erase all data pertaining to them, with a few notable exceptions. Grounds upon which a data subject may rely for an erasure request are as follows: (1) the subject's data is no longer necessary for its original collection purpose; (2) consent has been withdrawn and no additional basis for processing exists; (3) the data subject objects to processing via Article 21(1) or 21(2), and no overriding legitimate grounds exist for retaining the data; (4) the data was unlawfully processed; (5) the controller is obligated to erase by virtue of an EU or member state law to which it is subject; or (6) the data was collected in circumstances outlined in Article 8(1), which involves data collected from a child in relation to various online services such as online shopping.

Notable exceptions to a controller's obligation of erasure include exercising the right of free expression, as well as situations in which data processing is *necessary* "for the establishment, exercise, or defense of legal claims." Article 17(3).

Transparency Regarding Information (Articles 13–14)

While Articles 13 and 14 essentially provide data subjects another right under the GDPR, they are simply phrased as a transparency obligation on the part of the controller that applies to any data collected. Whenever your client collects data about someone covered by the GDPR, the items addressed in Articles 13 and 14 must be conveyed to that data subject—either immediately or within 30 days if received by a third party—unless the data subject already has the information.

This complicates privacy notices on websites because your clients could have different notice obligations, depending on how they obtained data. That being said, if your client has a website, it is definitely a good idea to include a link to the client's privacy notice on each and every page—because if data collection is occurring via visitors, that constitutes first-hand collection. E-commerce clients may consider including a pop-up at checkout that further explains the process. And because cookies count as well, a pop-up notification when a data subject first reaches your client's website may be prudent.

Additionally, the identity of any third party from which data is obtained must be disclosed. Thus, if data is obtained from a third party, the recipient must disclose to the data subject who it obtained the information from. And since that could get pretty dicey through a conventional privacy policy, it might be a good idea to work out a different process for that. But inasmuch as it would be possible to list the information in a privacy policy, (say, if your client only receives information from one additional source), the client could still include it in the privacy policy as well as whatever other method the client decides on for notification.

GDPR Recitals also make it clear that "transparency requires that information addressed to the public or to the data subject be concise, easily accessible and easy to understand," that "the data subject should be informed when the personal data are first disclosed to the [new] recipient [where personal data can be legitimately disclosed to another recipient]," and that none of this is necessary where the data subject already possesses the information. GDPR Recitals 58, 60, 62. This may seem daunting for clients to consider as they rewrite their privacy policies, but it is necessary, given the emphasis that the GDPR places on transparency.

Data Protection by Design (and Default)

"Data protection by design" is another one of those buzz-phrases in the GDPR that sounds more complicated than it is, but it still takes a substantial amount of work to implement.

Under Article 17, commonly referred to as the "right to be forgotten," data subjects have a right to force processors and controllers to erase all data pertaining to them, with a few notable exceptions.

GDPR Article 25: Implementation

Article 25 states:

> Taking into account state of the art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

While the content of Article 25 is not as complicated as it is verbose, the implementation may nonetheless be onerous. Inasmuch as technology and cost considerations are not outweighed by extraordinary risks to data subjects, your client is

required to do what it reasonably can to implement technical and organizational measures to protect data.

This article also brings up two other terms that could predominate your clients' Article 25 compliance efforts: *pseudonymisation* and *minimisation*.

Pseudonymisation

According to Article 4, pseudonymisation is "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information." This comes with a caveat that the "additional information is kept separately and is subject to technical and organizations measures [á la Article 25] to ensure that the personal data are not attributed to an identified or identifiable natural person." In other words, data is pseudonymized when the pieces needed to make it identifiable are kept separately in a secure manner. It is important to note that the GDPR still applies to pseudonymized data. In short, you must keep the pieces of information that would allow you to identify natural persons securely stored away from each other. This could be done via encryption in some cases.

Anonymization

Anonymity is not discussed in Article 25; however, given the questions that typically arise related to anonymity when the pseudonymisation topic is discussed, we will briefly mention "anonymization" here as well. *Anonymization* is not a term that you will find in Article 4 with the rest of the definitions—for good reason—because truly anonymous data lies outside the scope of the GDPR. However, Recital 26 does define what the GDPR has in mind when it comes to anonymous data; it is data that does not relate to an identifiable natural person. Thus, instead of reducing the chance of information being linked to a natural person, the identifying information is essentially scrubbed from the data when it is anonymized.

In light of technology today, ensuring that data is truly anonymous is a very high bar, but it is not impossible because fortunately, the GDPR does not require that it be absolutely impossible to identify someone from data for that data to be considered anonymous. Rather, the anonymity consideration takes into account "all of the means *reasonably likely* to be used." It also takes into account "all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of processing [note that collection is processing, as we touched on above] and technological developments." So if a data subject's virtually anonymous data could be identified by a certain method, but it was extraordinarily unlikely, highly expensive, and excessively time-consuming, then that data may still be considered anonymous. Anonymization is a process performed on data already collected, though. Therefore, the original collection and further processing (*i.e.*, the anonymity-inducing process itself) must still remain in compliance with the GDPR.

Minimisation

"Minimisation" is defined at Article 5(1)(c) as data collected being "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed" and is one of a number of principles established relating to the processing of data in Article 5. These next few mandates extend beyond minimisation to Article 5 more broadly, but your client needs to process only the data necessary and relevant to a particular, specified purpose, in a lawful and transparent manner. That data also has to be accurate, up-to-date, and kept in a form that allows identification only as long as necessary for the processing purpose, which is another way that anonymization can come into play. Your clients may also need to take a hard look at their retention policies. And of course, processing also has to be in a secure manner, which speaks to the prevalence of Article 25 measures.

Thus, your client's focus under Article 25 should be to develop and implement measures designed to protect the data that it processes. If your client has not looked at data security in detail lately, this may be a good time for them to implement more stringent protocols.

Does Your Client Need GDPR Representation?

If the GDPR applies to your client, there is a high likelihood that the client needs one or more types of GDPR representation in addition to yours.

GDPR Article 27 and 37: European Union Representative and Data Protection Officer

For clients that are not based in the European Union, Article 27 adds a wrinkle: a non-EU controller or processor must designate in writing a representative in the EU (essentially the GDPR version of a registered agent). There is an exception here for occasional processing that does not include any special categories of data, as well as public bodies. The representative must also be located in a member state where at least some data subjects whose information is being processed reside.

Your client may also require a designated data protection officer (DPO). Article 37, which contains the bulk of this rule, states that "[t]he controller and the processor *shall* designate a data protection officer" in any case where one of the following occurs: first, if any public body except a court acting in its judicial capacity is carrying out the processing, a DPO must be appointed. Second, if the core activities of the controller or processor require regular and systematic monitoring of data subjects on a large scale, a DPO must be appointed. Lastly, if the core processing activities of a controller or processor involve processing special data categories described in Articles 9 and 10 on a large scale, then a DPO must be appointed.

"Special" data is actually pretty commonplace, so more clients than you might expect could require designating a data protection officer. Any data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for purposes of identification), health data, or data related to sexual activity or orientation is considered "special" under Article 9. And any data concerning a criminal conviction or offense is also treated differently by Article 10. So entire *industries* are required to appoint a DPO within their organizations just by virtue of the "special data" categories above. All of that is to say that while your clients may not need a DPO, take a hard look at Article 37 and encourage them to consider the types of data

described in Article 9 before giving a definitive answer.

Security Breach Notifications

Articles 33 and 34, dealing with security breach notifications, are written in a straightforward manner, although they may be more complex in practice.

GDPR Articles 33 and 34: What They Mean in Practice, Briefly

Your controller clients' assessment of a potential security breach should proceed as follows under Articles 33 and 34:

1. Is there a security breach? If yes, continue to number 2.
2. Is the security breach likely to result in a risk to the rights and freedoms of natural persons? If yes, continue to number 3.
3. Clients have 72 hours to tell the regulatory authorities about it in the terms prescribed in Article 33 and proceed to number 4.
4. Is the security breach likely to result in a *high* risk to the rights and freedoms of natural persons? If yes, continue to number 5.
5. Tell data subjects about the breach without undue delay.

For processors, the key is to relay the existence of the breach to the controller without undue delay so that the controller can then fulfill its obligations as well. All of this is undoubtedly an oversimplification; however, the days of conducting a drawn out internal investigation before even considering telling anyone about a potentially serious breach are likely over for anyone within the reach of the GDPR. Clients will need to identify the bounds of a data breach quickly and be able to communicate swiftly to the data subjects about the breach, should that end up being necessary. Accordingly, clients may want to have a data breach communication policy mapped out proactively, ensuring that delays do not run afoul of the GDPR.

Transatlantic Data Transfers and How to Keep the Data Flowing

Year after year, globalization continues to show that the economies of individual nations are intertwined to an extraordinary degree. So it should come as no surprise that the GDPR has a global effect. That effect, however, would not be a positive one if it precluded the free flow of data from other nations to the EU and vice versa. That places the future of transatlantic data transfers between the EU and the United States at the forefront of your clients' considerations.

GDPR Articles 44–49: Bases for Transferring Data from the European Union

Chapter V of the GDPR goes into depth about transfers of personal data to third countries or international organizations. Possibilities for transferring data from the EU elsewhere must rely on one of several bases. These methods include an adequacy decision, a legally binding and enforceable instrument between public authorities, binding corporate rules, or standard contractual clauses. Articles 45–46. To be clear, these are only methods by which a data transfer itself may be deemed lawful; these are not ways to ensure compliance with the GDPR as a whole, nor are they to be confused with the bases for the lawful processing of data that we discussed above in connection with Article 6. An adequacy decision is when the European Commission determines that a nation has adequate data protection laws (on par with GDPR, now) and therefore may be considered a "safe" destination for EU-resident data. Given recent scandals in the United States involving data privacy, the United States may not be granted adequacy status as a nation until serious legislative changes are implemented; however, there is an agreement in place between the U.S. Department of Commerce and the European Commission called the EU-U.S. Privacy Shield through which American companies can self-certify. Self-certification awards the functional equivalent of an adequacy status to that company as long as it remains in compliance with Privacy Shield and the agreement itself remains in effect. However, while Privacy Shield certification makes the transfer lawful, note that it is *not* sufficient assurance for your controller clients when it comes to Article 28's requirements on the guarantees that they have to obtain from processor vendors.

Currently, your clients that need a lawful method of making these transfers probably need to self-certify as Privacy Shield compliant. However, that agreement is likely to be revisited by authorities in the coming days or weeks in light of a recent nonbinding vote from the European Parliament to suspend Privacy Shield as of September 1, 2018, if the United States did not fully comply before that time. While September 1 came and went without the agreement being pulled, there is still an annual review of the program that could affect the nature of the agreement before the end of 2018. Thus, beginning work on a contingency plan via one of the other methods is an important part of being prepared for life after the GDPR.

Compliance with the GDPR is a moving target and will likely remain as such until enforcement authorities solidify their interpretations of various provisions.

Conclusion

Compliance with the GDPR is a moving target and will likely remain as such until enforcement authorities solidify their interpretations of various provisions. While we have attempted to highlight a wide range of considerations and general rules, there is simply no way to include all of the requirements and exceptions contained in the 55,000-word regulation. That being said, if your clients begin implementing measures that comply with the points we have mentioned here, they will at least be moving in the right direction. The GDPR may sound overwhelming, but breaking down what the basic articles require and providing straightforward compliance recommendations will help keep your clients ahead of the GDPR enforcers. FD