GDPR Compliance—It Takes a Village

*Susy Mendoza**

INTRODUCTION

When the General Data Protection Regulation (GDPR) came into effect in May of 2018,[1] many legal departments were confronted with the gravity of just how they were going to comply with such a wide-reaching law. If you have international customers (both direct to consumer or business to business), it is not hard to convince your general counsel that compliance with the GDPR is a must. You may even be able to get the chief technical officer (CTO) or chief operating officer (COO) onboard just by mentioning the steep fines—two to four percent of worldwide gross revenue.[2] But how does the compliance message and method then trickle down to database administrators, product managers, software engineers, and enterprise architects? In order to get to the level of operational readiness companies strive for, it takes a village to facilitate moving the needle of regulatory compliance on any scale. In this Article I will chronicle what I have seen as building blocks in helping companies prepare for and execute on privacy initiatives.

I. EDUCATION

One of the most common questions I received in 2018 was "What is the GDPR?" Even with the elevated focus on privacy in the United States thanks to the well-publicized situation with Facebook and Cambridge Analytica,[3] understanding the impact of a European data protection regulation does not always reach the inner workings of an organization. In

* Director of Privacy and Technology Counsel at lululemon athletica inc. Many thanks to the Seattle University School of Law, and symposium participants.

1. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

2. *See id.* art. 83, at 82–83 (laying out fines).

3. Alix Langone, *Facebook's Cambridge Analytica Controversy Could Be Big Trouble for the Social Network. Here's What to Know*, TIME (Apr. 4, 2018 5:15 PM), http://time.com/5205314/facebook-cambridge-analytica-breach/ [https://perma.cc/J5BW-TX4E].

order to provide insight into why the legal department is now asking many questions about what information is collected in any one particular log file or with whom is the organization sharing employee data, each company should take time to lay the foundation and provide context to working groups and other internal partners.

The first challenge to overcome is boiling down the eighty-eight pages of the GDPR text into a format people will understand. Though there may be condensed, pre-packaged training available online, budgets may be tight for getting a larger organization licensed for a training as it may be licensed per user, which can rack up quickly in costs. Or it may be difficult to get the training actually viewed by those who are key to the cause. Since some of the difficulty with education is not only the breadth of a company but also the different perspectives each group may have, companies should try tailoring the training to specific tasks each division is responsible for.

For example, when speaking with a product manager, one may want to go over data capture and what actually needs to be collected rather than what the company would want to collect just in case, which aligns with the GDPR principle of data minimization.[4] With a database administrator or infrastructure team, it may be advisable to focus on the relief that comes from encrypting data at capture, transit, and rest.[5] At a smaller, more nimble and centralized organization, it may be possible to crowd everyone into the largest conference room and give a twenty-minute overview of the GDPR and its impact on the company, addressing specifics with individual groups in additional meetings. However, if one has a global company with several groups spread throughout the world, video conferencing could be an effective method of training. For those questions that come to the legal team frequently, use of a GDPR FAQ page on an intranet site may come in handy as well.

In addition to educating the organization on the GDPR, it may be beneficial to train personnel on the fundamentals of privacy as part of the organization's "Privacy by Design" efforts. Such training could encompass education on what constitutes personal information, lawful processing of data, and consent. It will help individuals understand that credit card information and social security numbers are still key pieces of personal information, in addition to device identification (ID), internet protocol (IP) address, and geolocation data. Introducing the concept of lawful processing could be next, describing the plan to understand where the company is processing data and why each of the elements of data is being processed, otherwise known as data mapping. Understanding lawful

4. GDPR, *supra* note 1, art. 5(1)(b)–(c), at 35.

5. *Id*. art. 32(1), at 51–52.

processing will set up the teams to understand why data mapping is key to preparation and how the teams can help, as they are the domain experts for platforms, software-as-a-service arrangements, or other applications.

Another key topic to cover is consent. Though one's organization may not often use consent as the lawful method of processing data —perhaps using legitimate interest or fulfillment of a contract instead— consent comes up so often that it is worth going over what constitutes consent for the GDPR. Further, if you are in other areas in North America, you may also want to cover the Canadian Personal Information Protection and Electronic Documents Act[6] or the upcoming California Consumer Privacy Act (CCPA).[7] Consent can be different within different regulations as well as when collecting different pieces of data (e.g., soft opt-in versus express consent). Consent is also key to some foundational marketing rules, both for those countries like the United States, which have opt-out rules,[8] and for those countries like Germany, which require a double opt-in.[9]

Once the background on what constitutes the GDPR and how it affects the company is established, the next challenge is communicating with individual groups about the part they play in making the company compliant with the GDPR. This may be the result of a gap analysis (discussed further below) or through due diligence on the part of internal and external counsel. Educating the teams on what steps are being taken at a higher level will help the interaction of teams among different departments, advancing the organization's overall compliance efforts. For example, having the enterprise architect in the same room as the digital marketers can help piece together the different locations of data collection. Again, there is a roadshow opportunity to provide transparency and gain alignment on next steps. Once everyone is onboard with what must be complied with, the next step is how compliance is going to be achieved.

II. BUDGET AND RESOURCES

In December 2017, the Paul Hastings Law Firm released a survey of 100 general counsel/chief security officers from Financial Times Stock Exchange 350 companies in the U.K. and 100 general counsel/chief security officers from Fortune 500 companies in the United States. The survey showed that only 10% of Financial Times Stock Exchange 350

6. Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).

7. California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1789.100–198 (West 2018).

8. 15 U.S.C. § 7704 (2012).

9. *Urteil BGH, 10.02.2011, Az. I ZR 164/09 – Double-opt-in-Verfahren*, KARSTEN & CHUDOBA (Oct. 02, 2011), http://www.karsten-chudoba.de/urteile-werbe-und-marketingrecht/urteil-bgh-10-02-2011-az-i-zr-16409-double-opt-in-verfahren/ [https://perma.cc/7ALW-9MK5].

companies are budgeting for the GDPR.[10] However, 94% of Financial Times Stock Exchange 350 companies say they are on track for compliance. In the United States, 98% of Fortune 500 companies considered themselves to be on track for GDPR compliance, yet only 47% of U.S. companies had set up a GDPR taskforce.[11]

In reviewing the results of the survey, one can appreciate the mismatch between perceived levels of compliance alongside the budget and resources actually necessary to become, and stay, compliant. Hiring a third-party consultant to perform a gap analysis takes money, and once that money is available and spent, those types of reports beget questions: Who is going to see that all the work gets done? Where does the budget live? The legal department, often seen as a cost center, does not always get the right-sized level of budget for the heavy lifting of compliance. But a gap analysis by a reputable third party is often a positive and necessary first step to a roadmap of executing the how-to of compliance.

However, a note of caution for those considering hiring a third party, either a consultant or external counsel: one should ensure the third party matches up with the company's type, specifically the risk tolerance and the method of facilitation for the company. For some of the company's internal partners, this will be the first time they interact with a third party on this topic, and scaring the internal partners into adherence may not be the way to get the best out of teams, though it may be for some organizations. Additionally, understanding the lengths the company can or will go to get to its own comfort level is a discussion to have with the third party prior to the engagement.

Once the gap analysis is complete, the tricky part comes—one must understand how much it will cost to narrow the gaps. Companies must budget for technology, not only the technology to track data to present a way for customers or employees to exercise their data subject access rights (DSAR)[12] but also the time and effort the tech teams will need to do the work. Many organizations have internal charges—if the legal team wants to get the infrastructure team to encrypt databases, there are costs associated with it.

Another issue may also be the prioritization of GDPR-related tasks over those the business needs for product releases. Relying on the education provided to the teams, plus the affirmation from an external consultant, companies should be able to at least have a conversation about

---

10. *Fortune and FTSE Companies Underestimate GDPR Compliance by May 2018, New Research Shows*, PAUL HASTINGS LLP (Dec. 15, 2017), https://www.paulhastings.com/news/details/?id=5ae5ed69-2334-6428-811c-ff00004cbded [https://perma.cc/56C8-WG48].

11. *Id.*

12. GDPR, *supra* note 1, art. 15, at 43.

how to get GDPR-related tasks into each division's roadmaps, which means sizing for such efforts and subsequently budgeting for those to be assessed.

Depending on the size of one's legal department, project costs can go beyond internal team efforts, including how to use technology to manage data mapping, consent management, additional security, and awareness. Costs can extend to additional administrative tasks, such as project management and outsourcing data protection addendum collection and negotiation.[13] Once data mapping (often known as one's Article 30) has been completed, the legal team now has a list of all third-party vendors with whom it shares data. Often, many contracts must either be rewritten or overridden by new GDPR-friendly terms. The ongoing tasks of tracking all the contracts that have been released and identifying if the third-party has responded, when the third-party responded, and if the third-party has competing terms—not to mention the negotiations—can be taxing on a smaller legal organization that still must complete its day job.

Enlisting the assistance of interns, paralegals, or junior lawyers to track data processing addendums (DPAs) may be the best way to check these tasks off the list of compliance to-dos. If one is fortunate enough to be able to afford it or has a smaller legal team with less experience regarding DPAs or privacy regulations, budgeting for outside counsel is also something to consider. Outside counsel may be a key advisor when tackling harder and more specific compliance decisions because there is so much grey area in the GDPR; outside counsel may work with the third-party consultant in conducting the gap analysis and perhaps even help prepare one's Article 30 compliance. Depending on one's organization, a company may want to go through a data protection officer (DPO) decision tree to determine if that is another element of the GDPR the company will need to comply with. If one does not already have a DPO, this is another expense to be considered—and again, it would be useful to discuss with outside counsel whether one may also need an additional DPO in Germany.[14]

With administrative, technology, internal, and additional third-party costs all estimated, and with education done (for the meantime), one will want to take the business case to the company's executives or board to allocate funds for the GDPR roadmap.

---

13. For a discussion of project management, see *infra* Part III.

14. Lennart Schüßler & Natallia Karniyevich, *Germany Is the First EU Member State to Enact New Data Protection Act to Align with the GDPR*, BIRD & BIRD (July 2017), https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr [https://perma.cc/3V49-9AHS].

III. PROJECT MANAGEMENT

Finding one has convinced the board or executives to provide funding for GDPR compliance and having educated some of the teams who will be involved, now comes the hard work. The bread and butter of compliance will partially be able to be completed in chunks (e.g., privacy policy updates, website cookie notices), and other parts will require time and multi-team coordination (e.g., future and past records retention). This is usually not something the legal team can handle themselves—in fact, most of the time it is quite the opposite.

Mature privacy programs or information security teams (say, teams who have already received their ISO 270001 or have adopted a NIST framework) may have already established a process to work with their IT partners. However, in start-up environments or those mid-sized companies who are in the infancy stage of setting up a global privacy program, companies now have the task of not only getting the work done for the GDPR but also deciding how to implement a working partnership with technology or engineering organizations.[15] As a matter of daily activity, the legal department does not often run projects but rather provides advice on specific topics. Therefore, getting an organization to execute on different tracks all toward one larger goal calls for program management and requires the department to lead in a way that is aligned with how the organization usually goes about its project management.

Enlisting the help of a project manager to facilitate the coordination of all the internal teams may be a necessity seeing as how legal departments may have to engage with a company's front-end developers on changes to the website or discuss data subject access requests with engineers or digital marketing teams to be clear on the anonymization of IP addresses. Then one will want to track all the legal department work that needs to be done, such as lining up an external DPO and updating email collection pages on websites or employee handbooks in various countries. Project management also lends a hand to the legal department by creating and facilitating transparency into what is getting done and what still needs to be done. It may also be a way to present back to the reporting committee, stakeholders, or executive team that the money they budgeted is being well spent. If one is working with a small or start-up environment, this may also be the best way to create awareness in how to instill that privacy and compliance need to be included in product, code, or future releases.

---

15. *ISO/IEC 27001 Family—Information Security Management Systems*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/isoiec-27001-information-security.html [https://perma.cc/5VRA-QKJM]; *Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/cyberframework [https://perma.cc/V22Y-GRP6].

IV. ONGOING COMPLIANCE

The GDPR is not only a preparation-heavy regulation; it inherently creates the requirement to remain compliant on an on-going basis. There are several administrative-level Articles that require the incorporation of privacy awareness into regular business activities, such as procurement, information security, and budgeting.[16]

Once one has managed to assess which third-party vendors require a DPA due to the Article 30 that one has prepared, now one must also implement a system by which a procurement department, or a smaller legal department, attaches DPAs for the new vendors that may be subject to the GDPR. Business-to-business companies may tack DPAs on automatically for any new contract being signed, or post the terms online as click-through agreements. Smaller or midsized companies may find that larger vendors they negotiate with will have their own DPAs and that implementing a one-size-fits-all DPA may be a challenge. The good news about the GDPR is that the controller–processor relationship is well documented, so many changes to DPAs will be risk-shifting clauses rather than the specifics of audits or breach notification.[17] Educating the teams doing preliminary negotiations and escalating when reaching sticking points can cut down on the time going back and forth in negotiations.

Privacy by Design is captured in Article 25 of the GDPR[18] and is one of the hardest concepts to grasp. It can be a good first step to reach out to one's information security team, which is a close partner with the legal and privacy teams, to facilitate and implement technical options to cover new processing activities. The information security team may already have processes in place to evaluate new technology coming into a company's architecture, which one may be able to piggyback on to serve as a framework for creating a privacy-focused process. If one's company is small or does not have an information security practice, one may want to see how to prepare for new technology purchases, different uses of data, or other new data processing activities to add to one's Article 30. As described above in Part I, different divisions within an organization who regularly collect, use, or store data as part of the function of the division need to be familiar with data minimization and must be familiar with when to reach out to the legal department when changes occur to the use of data. This education, the ongoing partnership with the information security department, and the DPO governance structure will help a company show its compliance with Article 25.

16. GDPR, *supra* note 1, art. 25, at 48; *id.* art. 28, at 49–50; *id.* art. 39, at 56.

17. *Id.* art. 28, at 49–50.

18. *Id.* art. 25, at 48.

When the GDPR came into effect, those U.S. companies lucky enough not to be subject to it sighed in relief. That relief was fleeting given the current California Consumer Privacy Act (CCPA), which is currently scheduled to come into effect in January 2020 and includes a twelve-month look-back period, impacting data from 2019.[19] Though not as heavy on administrative burdens as the GDPR can be, the CCPA and the GDPR are more similar than not in terms of transparency of organizations and access rights of data subjects,[20] with the CCPA going as far as prescribing how companies must provide consumers access to a link titled, "Do Not Sell My Personal Information."[21] The CCPA extends what seemed like a broad definition of data in the GDPR into any information that "is capable of being associated with" either a consumer or household.[22] For direct-to-consumer businesses, information being associated with a household appears to cover all marketing information. Data mapping exercises done for the GDPR will come in handy here as they can show the legal department where additional measures may need to be taken to comply with the CCPA, and where data subjects ("consumers" in the CCPA) access requests may be trickier. Even though the name implies that consumers are the focus, many would argue employees are also included given the broad definition of personal data in the CCPA, though there is still time for the California legislature to clarify the statute prior to it becoming effective.

CONCLUSION

The passing of the CCPA has shown us that the GDPR is not the end of privacy regulation reform; there are more changes to come. Laying the groundwork, though challenging, time-consuming, and sometimes costly, will facilitate not only the legal department's ability to be nimble when those new regulations do come through, but also will help other divisions within the organization. If one prepares a company to flex its muscles around teamwork, project management, funding, and transparency, an organization will be positioned to ride the wave of compliance with the regulations coming its way. All it takes is a village.

---

19. California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1789.100–198 (West 2018).

20. *GDPR/CCPA High-Level Comparison Chart*, PERKINS COIE (Nov. 2018), https://www.perkinscoie.com/images/content/2/0/v4/204145/2108-CCPA-Comparison-Chart-v.3.pdf [https://perma.cc/Z8SW-GV4G].

21. CAL. CIV. CODE § 1798.135(a)(1) (West 2018).

22. *Id.* § 1798.140(a).