A Project Management Approach to Data Protection Compliance

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Build.*** When developing a data protection plan with a project management approach, first take stock of what elements of your existing plan can be reused and what you will need to add.
- ***Make a plan.*** Within the project management framework, create a task-list, assign roles, make deadlines, and identify costs and outside resources needed.
- ***Communication.*** It is essential to keep communication open with the project management team. Have regular check-ins to determine challenges, revise deadlines, and understand general progress.
- ***Upkeep.*** After a plan is in place, continue to meet periodically to monitor and refine data maps, process inquiries and requests, and make updates as needed.

Corporate counsel have been scrambling to comply with sweeping data privacy laws like the European Union's General Data Protection Regulation (GDPR), which went into effect in May 2018, and the California Consumer Privacy Act (CCPA), which took hold on July 1 of this year. These are complex laws that require significant work on the part of multiple stakeholders, with no clear road map to compliance, and there can be eye-popping penalties for non-compliance.

In fact, some companies have curtailed operations rather than tackling these laws, giving up potential revenue opportunities. Others have chosen to apply these laws globally, preferring to treat most personal data similarly and leaning into the predicted proliferation of privacy laws. This article describes how the small law department of one global company embraced a project management approach to address the challenges presented by GDPR, CCPA, and the multitude of similarly comprehensive privacy laws expected to follow in their wake.

DHI's data story

When DHI Group, Inc. confronted these laws, starting with GDPR, it realized the legal department would have to rely on project management in order to achieve compliance. DHI has been a leading provider of career marketplaces since 1990, with three main platforms: Dice for technology professionals, eFinancial Careers for capital markets and financial professionals, and ClearanceJobs for professionals who have federal security clearances. It serves multiple markets located throughout North America, Europe, the Middle East, and the Asia Pacific region and has more than 500 employees located around the world. Almost all of its revenue is generated from online activities.

Given its digital footprint, DHI manages significant amounts of data, sourced and located all over the world, and does not have the option of just shutting down in certain markets in lieu of compliance. DHI needs to remain engaged at the highest levels of practice on data protection to preserve the all-important trust of its customers and stakeholders.

To comply with GDPR and then CCPA, DHI's legal department worked with key business stakeholders to develop a formal project management framework to keep track of the massive number of interconnected tasks and keep the project moving forward in a timely manner. While

challenging, this approach proved successful and will now be used to address future data privacy regulations that the business will have to comply with, as well as to complete other complicated legal tasks.

Why project management?

GDPR presented a special challenge to legal departments. Compliance would require integrating specific data protection practices into business offerings and building processes to address data subject requests. It required more than simple issuance of policies and contract updates: It required a true compliance program that would change business and legal practices on an ongoing basis. For many companies, it represented the first time the legal department would have to spearhead development and maintenance of a robust compliance program that would touch virtually all areas of the business.

CCPA proved similar in its demands. Superficial compliance would not be successful and would proliferate reactionary practices that, over time, could prove more costly to resources than simply doing it right in the first place.

Using a project management framework is a radical change for many small and mid-sized legal departments. But the technique, which other corporate departments rely on to accomplish tasks of all kinds, makes a lot of sense as law departments transform from transactional cost centers focused on speedy contract negotiations or litigation resolution to proactive, value-added legal operations producing tangible results. The new global data protection and privacy laws represent an opportunity to create a well-functioning, sustainable compliance program, one that top management will recognize as providing meaningful value to the company as a whole.

Project management also helps legal departments stay compliant with emerging laws on an ongoing basis, as more data is collected and individuals assert privacy preferences, as the regulations change over time, and as new regulations come into force. A single failure, such as not responding to a valid data subject request, represents a legal violation, and relying on an ad hoc process is risky, not to mention time-consuming. Building processes now will pay dividends later.

This article offers a six-step project-management process that not only ensures proper compliance with current data privacy laws, but also creates efficiencies that will benefit any company as it addresses new data privacy laws and other legal matters.

Step 1: Assessing project components

The first step in project management is taking a 30,000-foot look at the project parameters. The general rules for GDPR were announced well in advance of their going into effect on May 25, 2018, and DHI began its preparation more than a year in advance. Some other companies found it necessary to begin the process even earlier.

DHI first assessed the requirements of the regulation and set up initial calls to find out how its career platforms work when it comes to data collection, what data it had (including “dark data”) and where it was stored, what is done with the data, and where the company might have legal exposure. This initial assessment shed light on the potential impact of GDPR on DHI’s business and the rough cost to comply, and resulted in a road map of the path to compliance. Importantly, an outside law firm or consultant cannot provide an accurate assessment of either.

While companies necessarily face novel issues from time to time, one critical benefit of implementing a project management framework is that a company can incorporate its learnings and build on previous work. When DHI tackled CCPA with the same initial goals in mind, it was able to take a look at the commonalities between that regulation and GDPR in terms of what the statutes say, what they are meant to accomplish, and how they treat data. Handling the commonalities is relatively straightforward since a process is already in place to comply, and the remaining pieces become the roadmap for the new project. This crosswalk of commonalities and distinctions is a straightforward exercise that should be completed by counsel with experience in implementation.

Step 2: Identify tasks and bring the team together

Once an organization has determined what elements of past privacy laws can be reused and what new elements are needed, it can create a list of specific tasks and assign personnel to each, figure out what outside resources will be needed, and identify costs. Outside counsel often have a role to play here, advising clients of requirements and working with the in-house legal team to flesh out an early prediction of the processes and products that will be impacted by the law. This plan will inevitably evolve as other stakeholders provide feedback.

Data privacy and data management involve multiple stakeholders beyond the legal department and its outside law firms. Depending on the tasks involved, team members could include IT staff, web developers, marketers, data managers, product teams, HR, and more. In DHI's case, the group grew into a cross-functional team spread across multiple offices. It included representatives from all brands and functions, including product, technology, marketing, and legal, with team members based in London, Frankfurt, Singapore, Hong Kong, New York, Des Moines, Denver, and San Jose.

While companies necessarily face novel issues from time to time, one critical benefit of implementing a project management framework is that a company can incorporate its learnings and build on previous work.

Project management defined

What is project management? It is the practice of leading a team through a temporary project from start to completion. It has a specific deliverable that is dependent on a finite time period and budget and is outside of the scope of daily work.

The process includes several steps to enable the completion of the project, including forming a plan, defining a process, identifying the people involved and how they will communicate and collaborate, and creating lines of authority and implementation policies.

Project management has always been a technique used in business, but it began to be considered a profession in the mid-20th century. It uses many of the practices that are used in business settings every day. But the work is shaped by the objectives, schedule, and resources of a given project and therefore leads to a level of focus that is unique to project management. More recently, law departments have gravitated to a project management approach because it instills discipline and engenders effective planning, resource allocation, risk management, and cost control.

Typically, however, the legal representatives are the quarterbacks, directing the other departments on the regulatory requirements and approving or seeking modifications to their proposed implementation of the plan. Outside counsel can serve in this role with some success, but Wyrick has found that the effort is more fruitful when in-house counsel are engaged, in some cases simply to escalate concerns about participation by other business departments.

> **Ultimately, if company leadership is not motivated to support the project, it will not be successful. Therefore, strong advocacy by internal leaders, potentially backed up by outside experts, is essential. There is nothing like a CEO getting on a call to show how seriously the company views a project and to spur everyone on the team to commit.**

DHI convened its stakeholders in a kickoff meeting and conveyed the message that all team members would be held accountable for completing their assigned tasks. This early articulation of the basic plan and its criticality is essential for the project to be executed successfully. Plan for this meeting to be largely Q&A: Legal will need to listen to all stakeholders' concerns and generate support for the early project plan.

Forming a team for a data protection compliance project

Your data protection compliance project team cannot be comprised only of members of the legal department. It also must include representatives of the business departments charged with managing various aspects of compliance long term.

These members could include one or more members of the IT team, marketers, content generators, data managers, product managers, customer service personnel, and web and app developers, along with legal staff, and at least one C-level executive.

The team's roles in the company can encompass a range of titles, from less experienced staffers who will be managing the continuing documentation, correspondence, and scheduling, through mid-level managers who are responsible for implementing the systems needed for compliance, to senior management whose involvement underscores the importance of the project.

The team also typically includes one or more representatives from each geographic region impacted by a new regulation.

Step 3: Secure resources and buy-in

Support from the top levels of the organization is also key. In addition to DHI's chief legal officer

being a project sponsor, the chief executive officer and chief technology officer (CTO) were also enlisted as project sponsors. A product and technology specialist was appointed project manager.

Not all companies will have the CEO, GC, and CTO actively engaged, but their support is critical. For organizations still looking for that support, leveraging experienced outside counsel to provide insight on the dangers of noncompliance can be helpful. Speaking to actual experience with enforcement tends to be more effective than relying on headlines about significant fines, which may appear to executives to simply be a disproportionate scare-tactic. Similarly, experienced counsel should be able to advise on the business impacts of weak compliance, such as busted deals and audits by corporate customers.

Ultimately, if company leadership is not motivated to support the project, it will not be successful. Therefore, strong advocacy by internal leaders, potentially backed up by outside experts, is essential. There is nothing like a CEO getting on a call to show how seriously the company views a project and to spur everyone on the team to commit.

Step 4: Assign tasks, identify dependencies, and set deadlines

With leadership support and a list of tasks in hand, it is time to identify which need to be done first and which are dependent on the completion of other tasks. The activities on DHI's project roadmap plan for the GDPR project included data mapping and life-cycle analysis of the data, including collection, processing, storage, deletion, and end-of-life destruction.

Start and end dates can then be locked in for each task and a master schedule completed. After determining the best person to perform each activity and inviting each team member to join the group, assignments can be made. At this stage it is important to think several steps ahead: What tasks are dependent on other tasks? If website development resources are needed at a later stage but likely to be constrained, how can you work backward from the deadline to ensure all dependent steps are executed in time to implement website changes? Meeting with the larger team regularly to assess status, accuracy, and completeness of tasks, and identify roadblocks, is essential.

The project plan was an evolving document to which the team regularly added or revised tasks and dependencies. Here again, experienced practitioners can be helpful because they will have encountered unforeseen roadblocks with clients that were earlier adopters of project plans and can therefore help new clients navigate. In-house resources should also be utilized fully. For example, technologists often come to the table with project management experience using software development methodologies such as Agile or Kanban. Incorporating these frameworks can help engender trust and build credibility.

Using the project management approach developed for GDPR, and taking time to examine commonalities with CCPA upfront, was a real advantage for DHI when it came to scheduling the CCPA project. DHI established an aggressive plan to come into compliance well in advance of the law' effective date and was able to stay ahead of that schedule.

Step 5: Ensure communication and team-building

Setting up a proactive process for regular communication among team members, whether they number three or 30, is essential right from the start of the project. Regular check-ins allow team members to discuss changes in plans, roadblocks or challenges that come up, or general progress.

There may be a need to revise the plan over time, and deadlines may need to be adjusted. There also must be a mechanism for raising red flags, whether they are warnings that need immediate action or less urgent heads-up notices about potential problems ahead.

DHI scheduled hour-long video meetings every other week, starting a year before the GDPR compliance date. Team members could tap each other as resources, discuss needs, and identify issues that required liaising with outside connections and stakeholders. Six months out, as the team grew, the schedule was ramped up to every week, and three months out ramped up again to twice weekly.

While not a core challenge for DHI, it is important to have knowledgeable delegates engaged so that the absence of one key player in a given week does not derail the process and side issues are addressed in a timely manner. For example, outside counsel may not be able to spearhead the primary monthly calls, but can cover side meetings that may emerge, if in-house counsel are otherwise engaged.

> **Setting up a proactive process for regular communication among team members, whether they number three or 30, is essential right from the start of the project.**

Some of the conversations that come up in team meetings can be stressful. Most stakeholders already have “day jobs” keeping them fully busy and they may resent a legal project encroaching on their time commitments. Here, executive buy-in and outside counsel’s reassurance that competitors are having to do the same (or should be) is valuable. Task-oriented meetings help foster accountability since participants generally do not like to report they have missed deadlines to a group audience.

GDPR vs. CCPA: Commonalities and differences

Both GDPR and CCPA have certain key provisions in common, meaning that companies that are already compliant with GDPR will have some processes in place that will help them adhere to CCPA as well.

For example, both laws dictate that individuals have the right to see the personal information companies have collected about them and request its deletion. Both also ensure companies are transparent about the information they have and how they use it, as well as requiring implementation of security measures. Both laws require companies to have contracts with service providers with regard to the use of personal data.

Beyond that, there are several differences between the two laws:

- **GDPR protects persons in the European Union, and CCPA residents of California.**
- **GDPR covers companies that have an establishment in the European Union or intentionally target or track persons in the European Union and process personal data, while CCPA is narrower, covering only companies that meet enumerated thresholds.**
- **Both require privacy policies, but the disclosure and update requirements differ.**
- **CCPA has a “Do Not Sell My Information” option for consumers, which GDPR does not have. GDPR has other unique individual rights such as data portability, rectification, and objection to processing.**

- **The penalties for violations and enforcement mechanisms are different.**
- **GDPR restricts data transfers that would provide access outside the European Union, while CCPA does not.**
- **CCPA's definition of personal data is much broader than GDPR's so companies must be able to locate and offer access to a longer list of data. CCPA also has specific verification requirements before individual requests are honored.**

This list just touches on the components of these complex laws. But it foreshadows how the data protection laws expected to fall into place around the world in the coming years are certain to have their own requirements, necessitating a unique approach to compliance. That said, all are also likely to have certain elements in common with other regulations, allowing companies to build on past efforts and making the case for utilizing a project management approach.

One of the goals of setting up a project management framework for compliance with new privacy laws is to simplify the process of complying with future laws by leveraging past work. To do this, it is important to take the time to assess what worked well and what could be improved, and to tweak the process if needed.

It is also important to keep the meetings moving along. No one member of the team should sideline the group with extended discussion of issues; any concerns that might bog down the meeting can be addressed offline. The legal department quarterbacks the call and ensures that roadblocks are identified and diverted to separate, smaller group meetings. A project manager recording minutes, updating to-dos in real time during the calls, and pursuing follow-ups also contributes to an efficient meeting.

In addition to the regular meetings, the project team should have access to shared documents. DHI's stakeholders did so through its company project collaboration tool. This gave all participants the ability to contribute, share, and be informed of real-time status updates on activities completed as part of the project roadmap.

Over time, the regular check-ins, collaboration, and real-time shared updates made all team members feel like their voices were heard and that they were important to the project. Having leadership and external experts set a "we're all in this together" tone is also critical for success. In DHI's process, team members were able to check their egos at the door and realize that all the work was geared toward the team getting to the finish line. With momentum building throughout the project, what may have started out as a "no glory" assignment to some on the team ultimately transformed into a significant team achievement with all members contributing. This mentality is arguably the most important ingredient to generate momentum and, ultimately, deliver long-term success.

Step 6: Review for process improvements and sustainability

One of the goals of setting up a project management framework for compliance with new privacy laws is to simplify the process of complying with future laws by leveraging past work. To do this, it is important to take the time to assess what worked well and what could be improved, and to tweak the

process if needed.

After the GDPR compliance deadline passed on May 25, 2018, the team was given a week off for a breather before being invited to a post-mortem of what went right and wrong and where the system was getting bogged down. The meeting helped hone and improve the process to ensure it worked smoothly when CCPA came around. An added benefit was that soliciting team members' input made them feel as if they were part of something bigger and that their contributions would be valued going forward. It also helped foster a "best practices" approach to the work of the members of the team.

A smaller team continues to meet periodically, charged with monitoring and refining the data maps, processing inquiries about data, addressing data subject access requests, and providing company-wide training. A senior lawyer and the company data protection officer check in regularly to liaise with the team, particularly as rules are adjusted or as new data inquiries come in.

Key takeaways

Complying with the new, complex data privacy laws, which put more power into individuals' hands than in the past, can seem overwhelming. The project management structure DHI set up to address GDPR created a frame-work that puts the legal department in a position to continually improve best practices, comply with laws, and evolve over time. That framework streamlined and sped up CCPA compliance efforts.

Developing, implementing, and using a project management framework does not have to cost a lot. At DHI, team members on both the GDPR and CCPA projects were already employed by the company, and the collaboration technology was already in place. The framework created efficiencies that helped use resources efficiently; for example, the team was able to reach out for outside counsel and other third-party assistance only when necessary, which kept costs down. DHI's incremental cost, even on a project with the magnitude of GDPR compliance, was nominal, and that was a win for the legal department.

Importantly, the framework is scaleable, repeatable, and flexible. It can be used not only for new data privacy laws that will continue to be implemented around the world or for projects as diverse as M&A transactions, litigation matters, and making a smooth transition from on-site to remote work situations and back again during COVID-19.

A project management framework and its successful implementation also communicates to the C-level that the in-house legal function can generate ideas that provide value to the company and that it can, by planning for the project and bringing in stakeholders with accountability, implement those ideas while managing the company's legal matters.

With the implementation of compliance frameworks for GDPR and then CCPA, law departments have been driving projects within their company in a meaningful way. Typically business departments spearhead the projects and must reluctantly bring in the legal team — viewed as the "department of no" — for a review. A project management focus changes this dynamic. The legal and business teams become equal partners, the relationship between the two is a positive one, and important things can be accomplished. That is a big win for everyone.

ACC EXTRAS ON… Data protection

Cybersecurity in the Age of COVID: How to Protect Your Data (Aug. 2020). accdocket.com/articles/cyberthreats-age-of-covid-19.cfm

Privacy Now: A Dedicated Data Discussion (Jan. 2020). accdocket.com/articles/resource.cfm?show=1505351

One Year After GDPR: How Are Legal Departments Handling the New Data Policies? (May 2019). accdocket.com/articles/one-year-after-gdpr.cfm

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT WWW.ACC.COM, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

Brian Campbell

Chief Legal Officer

Trajector

Brian P. Campbell is the chief legal officer of Trajector, which he joined in March 2024. Prior to joining Trajector, Campbell served as chief legal officer and corporate secretary of DHI Group, Inc. (NYSE: DHX). Campbell joined DHI as its first general counsel in January 2000 and served as chief legal officer/general counsel and corporate secretary of DHI Group until September 2023. Prior to joining DHI Group, Inc., Campbell served as vice president, general counsel, and corporate secretary at CMP Media (NASDAQ: CMPX), where he worked since 1995. From 1988 to 1995, Campbell worked as a corporate associate in the New York office of the global law firm of Mudge, Rose, Guthrie, Alexander and Ferdon.

Campbell serves on the global Board of Directors of the Association of Corporate Counsel (the “ACC”), where he is a member of the Advocacy Committee and the Cybersecurity and Risk Committee, as well as Chair of the Technology Advisory Committee of the Board. He is a past chair of the Small Law Department Network of the ACC and is a past president of the New York City Chapter of the ACC, where he served on the Board of Directors for six years and has

been a member for over twenty-five years. Campbell is also a Charter Member of TechGC, a peer community of general counsels of technology companies.

As a recognized leader in the in-house legal community with over 23 years of chief legal officer/general counsel experience, Campbell regularly addresses critical in-house topics as a frequent author, speaker, and panelist for publications and events.

Elizabeth Johnson

Leader of the Privacy and Data Security Practice Group

Wyrick Robbins

Elizabeth Johnson leads the Privacy and Data Security Practice Group at Wyrick Robbins, a member of Meritas Law Firms. Her experience includes compliance initiatives for CCPA, GDPR, HIPAA, and other privacy laws, data breach response, and response to regulatory reviews.