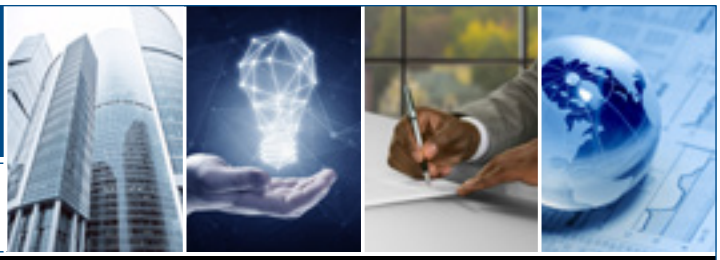
ALSTON & BIRD

WWW.ALSTON.COM



Privacy & Data Security ADVISORY ■

SEPTEMBER 28, 2018

Applying GDPR Process Lessons to the CCPA

By Jim Harvey and Karen Sanzaro

The California Consumer Privacy Act of 2018 (CCPA)[1] will become effective on January 1, 2020, and though the CCPA was hastily adopted and remains subject to further amendment,[2] most companies will need to commence compliance efforts now. The timing of the CCPA's introduction and adoption in June – just after the May 25, 2018, effective date of the European Union's General Data Protection Regulation (GDPR) – naturally invites comparison with the GDPR, though the scope and content of the California legislation is quite distinct from the GDPR. That said, recent experience with GDPR compliance implementation efforts offers invaluable insights in preparing for the CCPA. Many companies subject to the GDPR have already implemented core data governance and privacy process changes that will likely give them a head start in implementing the CCPA. For other U.S. companies, the CCPA will present their first major privacy and data governance initiative.

We will not examine the purely legal aspects of the CCPA, which have been and will continue to be examined elsewhere.[3] Rather, we will focus on lessons learned from the GDPR compliance process that should prove helpful to companies struggling with major privacy and data management requirements for the first time. These lessons include the importance of a robust data inventory, the role of consultants and compliance systems, required collaboration across the organization, and vendor management.

---

1 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.198(a) (2018).

2 Unlike the GDPR, which went through an extensive comment process, the CCPA was adopted in record time and consequently remains subject to amendment before the effective date. Despite the possibility of those changes, the core of the statute will likely remain in place. See https://www.alstonprivacy.com/california-legislature-amends-ccpa/ for a summary of the August 31 amendment.

3 *See, e.g.*: Privacy & Data Security Advisory: Landmark New Privacy Law in California to Challenge Businesses Nationwide, by David Keating and David Caplan; California Legislature Amends CCPA, by Michael Young; An Update on the California Consumer Privacy Act and Its Private Right of Action, by Gillian Clow.

Lesson 1: Leadership and Multidisciplinary Collaboration. Executive support and a multidisciplinary team is essential to a successful implementation.

It was readily apparent during the early stages of companies' GDPR compliance efforts that implementation of the overarching data privacy practices introduced by the GDPR would require a collaborative, multidisciplinary team – with strong leadership. The requirements imposed by the CCPA are, similarly, too extensive to be addressed with "paper policy" changes alone, and too complex and overarching for individual business units to develop isolated compliance approaches.

While the effort is a response to a new law, the process for achieving compliance with the CCPA should not be viewed or managed solely as a legal endeavor. Like the GDPR, the CCPA will require an assessment – and possible overhaul – of many technical and organizational processes involving personal information (which is extremely broadly defined under the CCPA).[4] The potential long-term impact of the CCPA on the business (and the information systems that support the business) necessitates an interdisciplinary and collaborative approach.

Determining ownership within the organization and acquiring resources from multiple groups within the organization to successfully implement the CCPA will be a significant endeavor. Most successful compliance efforts are the product of a strong leader (supplemented by a small group of lieutenants, if needed, in larger, more complex organizations) appropriately situated within the organization. This person should have a clear mandate from the executive suite in order to avoid being perceived solely as a compliance, IT, or legal functionary without the appropriate organizational support to execute on a large and diverse project.

Lesson 2: Budget. Budget appropriate funds for your CCPA implementation as soon as possible.

Budgeting for the extensive efforts required to comply with the GDPR was a bit of a hot potato for many companies. The impact of the GDPR compliance effort within organizations was wide ranging – encompassing various cost centers that extended well beyond legal and complicating the budgeting process.

While the budgeting allocations for the CCPA effort will necessarily be specific to each organization, the lesson learned from the GDPR is to tackle this issue sooner rather than later so that the CCPA implementation effort is not derailed or delayed by internal conflicts. There is no time to waste, as most organizations will have to start the compliance effort in 2018 to assess and implement the many likely IT and business process changes required by the January 1, 2020, effective date.

---

[4] "Personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" and specifically includes IP addresses, purchasing histories, geolocation data, Internet search histories, and consumer preferences or profiles if they can identify or be reasonably linked with a particular consumer or household. CCPA, §1798.140(o)(1).

Lesson 3: Data Inventory and Mapping. A good data inventory and map is essential to compliance efforts – and extremely time consuming.

The CCPA will require companies to track data of California residents within their enterprise, provide information about that data to those residents, and track and control the disposition and use of that data within and outside their organization. While it seems self-evident, the GDPR implementation process confirmed what privacy and data management professionals have long asserted – that in order to properly implement a significant regime change for management of data, companies must first understand what data is collected, from where or whom the data is obtained, what systems process the data, where those systems are located, to whom data is transmitted, and for what purpose.

While the size and complexity of an organization – and the extent of its reliance on consumer data – will impact the difficulty entailed in this task, a comprehensive data map and inventory has proven to be more challenging than anyone could have expected. There are technological tools that can assist with the identification and mapping process; however, the process will require a significant investment of person hours, management energy, and knowledge of the company's data practices and the underlying compliance requirements to render effective results. The point of the exercise is to understand what personal information resides within the organization, its sources and uses, and the internal and external systems that process it. However, the CCPA will also likely require some changes to the implicated systems and business processes.

Understanding the data landscape is a necessary first step in the compliance effort – only then is it possible to identify the nature and extent of changes that will need to be made to the systems and business processes that make up that landscape. While it may be possible to retrofit the relevant databases, systems, networks, and business practices, attempting to change the data landscape in any fundamental manner without first understanding and documenting it may lead to significant pockets of data and issues being overlooked, resulting in noncompliance or the need to re-engineer processes and/or systems as mistakes are discovered.

Though painful and time consuming to generate, a well-crafted data inventory can serve multiple purposes. It provides the initial foundational understanding on which the compliance effort is managed, but can also be used to demonstrate and track compliance on an ongoing basis. It can be integrated with an organization's privacy by design / privacy impact assessment processes so that new data initiatives, or material changes to existing practices, are also evaluated and tracked.

Lesson 4: Consultants and Third-Party Compliance Tools. Be strategic in your use of third-party consultancies and compliance programs.

Most companies will inevitably turn to outside consultants to assist with various aspects of implementation of the CCPA, whether because of a lack of expertise or bandwidth, or both. This was certainly the case with the GDPR, where we saw vastly different consulting relationship outcomes. It is crucial – for the CCPA and any major compliance effort – to stay involved and actively manage consultants (including outside lawyers). As we noted in Lesson No. 1, appropriately authorized leadership – with executive-level support – is the first step to success. As a general rule, we have found internal leaders – with the necessary relationships and corporate knowledge – to be more successful. That said, with appropriate diligence and ongoing management, outside resources – including technology solutions – can prove invaluable.

When engaging outside consultants for a CCPA compliance effort, take into account both the strengths and weaknesses of the consultant and how those dovetail with the gaps you are trying to fill. While there are certainly advantages to one-stop shopping for consultants, consider whether your organization may be better served by a more targeted approach. For example, employing one consultant for the data mapping and process design and another consultant to implement the recommended system changes may help avoid potential conflicts of interest. It also allows greater flexibility in choosing the best fit and expertise available for each phase or work stream of the compliance effort.

This holds true for third-party technical solutions as well. We have seen a wide range of technology products marketed as GDPR-compliance tools. Some very targeted – for example, managing consumer marketing preferences – and some more comprehensive, with multiple modules and seemingly endless options. In selecting compliance tools, it is important to understand your organization's actual requirements, narrow your options accordingly, and then do the necessary diligence to determine the best fit. These tools are just that – tools to assist in managing compliance. They are not an alternative to a robust compliance implementation process. Given the newness of the CCPA, if you are contemplating using a third-party technical solution, be sure that the capabilities being touted are actually available, and not just on the roadmap. Or, alternatively, if your organization will be an early adopter and influencer, be sure that the contract (and pricing) reflects this role – and that you have the necessary internal or consulting resources available to provide the required input.

We often encounter questions about what consultants should do in major privacy and data implementation projects as opposed to lawyers. Indeed, depending on the circumstances, it is quite possible that use of consultants will far outpace the use of lawyers. At the end of the day, the two groups have to be coordinated with one another, and this coordination will inform and improve the performance of both. Lawyers should not be engaged heavily in purely business endeavors, as that will not leverage their legal skills and insight. However, they should also not be so far removed from the business that their advice is rendered out of context, or provided merely as guideposts for the business to go off and implement on its own. Likewise, consultants should not engage in purely legal endeavors – their business process implementation should be informed at every stage by appropriate legal analysis made by lawyers well-versed in both the CCPA and your business.

Lesson 5: Vendor Management. Include and initiate a "vendor management" work stream early on in your compliance effort.

As the data-mapping process will reveal in stark detail, most organizations rely on a vast network of third-party relationships – ranging from service providers, marketing partnerships and co-branded relationships, data brokers, and others. Similar to the GDPR, the CCPA will require organizations to identify third parties with whom personal information is shared, disclosed, or sold and, in some cases, to pass along consumer requests regarding their data to such third parties or otherwise coordinate with third parties about notices, opt-outs, and consumer data rights. Additionally, the CCPA requires particular language in agreements with third parties and service providers in order to avoid a "sale" of personal information under the statute, and

it provides certain liability safe harbors if the agreements are structured properly.[5] All of this underscores the importance of assessing your third-party and service-provider agreements and likely amending a significant number of them.

Identifying these relationships – and determining how to address the compliance requirements – will be a significant challenge, one that is made more complicated given the inherent dependency on third parties, many with little incentive (other than the continuation of business) to engage in the process. Given the challenges and dependencies, it is crucial to allot sufficient time in the compliance effort to assess third-party relationships, develop a compliance approach for both new and existing third-party relationships, and implement that approach for existing relationships (often based on an internal assessment of risk and priority).

---

5 *See* CCPA, §1798.140(t)(2)(C); CCPA, §1798.145(h).

You can subscribe to future ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Jan Dhont
+32 2 550 3709
jan.dhont@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM