

America's GDPR?

*Seven workstreams to
implement California's
Consumer Privacy Act*

Table of contents

America’s GDPR? Seven workstreams to implement California’s CCPA	1
<hr/>	
Workstream 1: Privacy policy management: Update privacy notices and policies.	1
Workstream 2: Data lifecycle management: Update data inventories, business processes, and data strategies.	1
Workstream 3: Individual rights processing: Deploy rights to access and delete and stop selling data.	2
Workstream 4: Privacy by design: Embed privacy design requirements and PIAs.	3
Workstream 5: Information security: Close medium-risk gaps.	3
Workstream 6: Data processor accountability: Update service-level agreements.	4
Workstream 7: Training and awareness: Deploy role-based training and change management.	5

Seven workstreams to implement California's CCPA

The California State Assembly's June 2018 passage of the [California Consumer Privacy Act](#) (CCPA) promises to generate a tsunami of corporate privacy initiatives across all sectors until its January 2020 deadline. PwC clients that deployed against the EU's General Data Protection Regulation (GDPR) with our 10-workstream model will have a head-start addressing seven of these workstreams that CCPA affects. But retailers, financial institutions, and other sectors that are primarily focused on the North American market and largely escaped GDPR's scope will probably face the largest data privacy mobilization in their companies' history. Companies in all industries will need to make strategic decisions on whether to offer these protections only to California residents, and to what extent they will rely on exceptions and carve-outs in the legislation that may not be clarified by the State of California until January 2020.

Workstream 1: Privacy policy management – update privacy notices and policies

The [California Online Privacy Protection Act of 2003](#) already requires companies that process personal data of California consumers through commercial websites to post a privacy notice there. Companies hit by GDPR had to add detail to those notices.

CCPA resurrects this drill. The new law mandates that companies provide notice to consumers and employees indicating the categories of personal information collected and the purposes for which they are used. The notice must explicitly indicate the categories of their personal information that are collected, disclosed, or “sold” -- using a broader definition of “sold” than seen before -- and that they have a new right to opt-out of this selling. Companies may not collect additional categories of information or use information for additional purposes without providing consumers with an updated notice. Similarly, companies will need to update their privacy policies to include a description of the other new consumer rights afforded by the CCPA.

Before making these updates, companies will need to step back and determine if they will maintain one privacy notice for California residents and one for everyone else, or stick with one unified notice.

Workstream 2: Data lifecycle management – update data inventories, business processes, and data strategies

Data inventories. Article 30 of the GDPR famously requires companies to maintain a “record of data processing” -- or “data inventory” as we call it in America. While CCPA does not explicitly require companies to maintain a data inventory, it will be practically impossible for companies to comply with CCPA without one. Companies will need a database that tracks all the business processes, third parties, products, devices, and applications that process California residents' personal data and keep it up to date as all of these things change.

Multinationals hit by GDPR will have a jump start on this requirement. They will have designed the database, populated it with metadata about systems processing data about EU residents, and assigned responsibilities to the first and second lines of defense to maintain this record.

Even the most mature data inventories, however, will need an upgrade to meet the unique aspects of CCPA. Three additions might generally be needed: a column flagging whether a data-use case involves data “selling”; a tracking of the categories of personal data transferred to third parties; a column indicating whether the data was only collected more than 12 months ago and therefore potentially exempt; and a column indicating which data categories are covered by pre-emptive federal legislation such as HIPAA, GLBA, and FCRA that might also exempt the data from coverage.

Once these mature data inventories are updated, the privacy offices responsible for them will need to launch a campaign with their privacy champions and data stewards in each corporate function and line of business to populate these new fields.

Business processes. Deploying and updating data inventories might be the more straightforward initiative under the data lifecycle workstream. The larger operational impact is likely to be re-engineering business processes to function effectively once California residents start expressing their rights to opt out of data selling and to delete their data. Some processes that inherently “sell” data will need to be either discontinued or unwound so that opted-out consumers can continue to be served. Other processes that depend on consumer transactional data will need the “delete” action designed so that system-critical, de-identified data is not also deleted.

One of CCPA’s most unique requirements may also prove to be its largest market disruptor. CCPA prohibits companies from offering lower service levels to consumers who’ve expressed their CCPA rights. This affords companies the ability, however, to “offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer’s data.” This caveat gives a large incentive to companies to galvanize their economists to model the value of consumer data relative to their goods and services.

Data strategies. Taking these data-governance requirements together, companies that overhaul their business-data strategy and engineer their revenue-producing business processes around this strategy could make market-disrupting gains while their competitors are taking a minimum-compliance approach.

Workstream 3: Individual rights processing – deploy rights to access and delete and stop selling data

Companies covered by the U.S. Health Insurance Portability and Accountability Act (HIPAA) are familiar with its GDPR-like patient right of access. But few American companies operating outside the healthcare sector are equipped to offer this expansive right, let alone the more impactful rights to delete and stop data selling.

Here’s what the new law requires:

- *Right of data access.* Similar to the GDPR’s Article 15 - Right of access, CCPA states that consumers “shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.”
- *Right of data erasure.* Unlike the GDPR’s Article 17 - Right to erasure, the CCPA affords consumers a broad license to request deletion without formally withdrawing consent for processing or satisfying any other contingencies. It states consumers “shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”
- *Right to stop data selling and disclosure.* Unlike GDPR’s Article 18 - Right to restriction of processing, where certain conditions must be satisfied to restrict processing, California consumers are given plenary authority to terminate the sale of their information. It states: “A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information. This right may be referred to as the right to opt out.”

In order to comply with the prescribed timelines for these individual rights requests, companies must disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer.

To comply with these new rights, businesses will need to build effective request-management processes. Rollouts of this nature typically will include these steps:

1. *Documenting “data-subject request” (DSR) procedures* including how to authenticate requestors and appropriately deny out-of-scope requests, and which templates to use in responding to verified requestors;
2. *Defining “systems of record” (SORs) and “designated record sets” (DRSes)* that will be the authoritative sources of personal data from which the DSR responses will be based;
3. *Updating ticket-management and contact-center applications* to accommodate and track the fulfillment of the DSRs within the prescribed timeframes;
4. *Training first-responder staff* on the procedures and application changes; and
5. *Testing the efficacy of the new controls* before the January 2020 go-live date.

For those companies that spent the last two years implementing DSR measures under GDPR, the work ahead will amount to extending certain GDPR capabilities into the American market, and then adjusting certain processes to accommodate CCPA’s unique features. For everyone else, deploying individual privacy rights will be a drill they will want the full 17-month grace period to be able to get right.

Workstream 4: Privacy by design – embed privacy design requirements and PIAs

The GDPR also famously requires covered organizations to build in privacy-friendly default settings to their new products, services, and technologies, and to complete data protection impact assessments (DPIAs) in certain scenarios involving the processing of European personal data. Although CCPA doesn’t include an explicit privacy-by-design (PBD) requirement, it will be almost impossible to stay in compliance with the new law without a similar capability in place.

What does a “minimum viable” PBD function look like for CCPA? It’ll contain two components: privacy design requirements (PDRs) and privacy impact assessments (PIAs).

- *PDRs.* Privacy offices of companies who serve California residents will want to galvanize their privacy champions in each corporate function and line of business to help them define PDRs for their business processes, systems, products, and services. PDRs are privacy standards that define default settings related to the collection, use, and disclosure of personal data and the enablement of the DSRs described above in section 3.
- *PIAs.* Like their GDPR-cousin DPIAs, PIAs are questionnaires that staff in the first line of defense -- the line of business and operational functions like marketing -- have to complete every time they deploy a new technology or use of personal data. The purpose of PIAs is to flag potential deviations from the corporate privacy policy in the design phase in order to correct the deviations when doing so is the least costly and impactful to the business. Fortune 500 companies with mature PIA functions easily complete hundreds of PIAs each year.

Workstream 5: Information security – close medium-risk gaps

The CCPA, like the GDPR, requires covered businesses to protect personal data with “reasonable” security. The Federal Trade Commission’s enforcement of the FTC Act similarly holds companies accountable to providing a reasonable standard of due care for the protection of personal data.

In practice, this “reasonable” standard has led companies to take a risk-based approach toward addressing threats to the confidentiality, integrity, and availability of personal data. They assess the threats to data, rank the risks of the detected vulnerabilities, and address the high-risk gaps first. For not a few corporations, the cost of addressing high-risk gaps is staggering, and some accept the risk of not mitigating some medium-risk gaps.

How does CCPA change this formula?

CCPA escalates the cost of not remediating a gap. As a result, the new law lowers the break-even point where it is cost-effective to fix a security gap. Once companies perform the economic analysis of the new law, more are likely to conclude their break-even point falls within the low-risk category of vulnerabilities and compliance gaps.

What are the CCPA penalty thresholds?

If “nonencrypted or nonredacted” California consumer information is compromised through a breach or some other unauthorized disclosure resulting from a failure of reasonable security, consumers may bring a legal action for statutory damages ranging from \$100 to \$750 per violation or actual damages, whichever is greater.

All other CCPA penalties are driven by the California Attorney General’s (“AG”) office. While the AG may also target the reasonability of a company’s security measures, it is responsible for pursuing statutory penalties across the entirety of the CCPA. Those penalties can reach \$7,500 per violation.

The CCPA defines strict timetables for consumers bringing class actions and for the AG to prosecute. It also establishes a Consumer Privacy Fund to use a portion of the proceeds from these settlements to offset court and AG costs of enforcing this law. California gave America and the world data-breach notification in 2003, and the CCPA anticipates a similar, wide-ranging ripple effect starting to spread from Sacramento in January 2020.

Workstream 6: Data processor accountability – update service-level agreements

Most large corporations maintain some level of a third-party risk-management (TPRM) capability for vendors and other third parties that process data on their behalf. These functions usually include standard-contractual language, vendor inventories, due diligence questionnaires, and onsite assessments. Companies impacted by GDPR may also be requiring their third parties to provide their records of processing, complete DPIAs, and sync with their DSR-response processes.

To get ready for CCPA, companies serving California consumers and employing Californian residents will want to do all of this and go one step further: to map the specific data elements shared with each third party, and a designation of which of this transfers would qualify as “selling” under CCPA. For the latter relationships, companies will need to design processes to accommodate consumer requests to opt out of this selling and to delete their data. This may involve dozens or even hundreds of conversations and working sessions with third parties over the next 17 months.

Companies acting as service providers to clients covered by CCPA will want to prepare for this approaching avalanche of inbound client requests. A win-win outcome for both sides of the data-processor equation will be the documentation of updated service-level agreements for each new CCPA requirement affecting the supply chain, and a negotiation of impacting cost and pricing arrangements.

Workstream 7: Training and awareness – Deploy role-based training and change management

CCPA will bring enormous system and business-process changes to most companies operating in California. It will change the way many people do their daily jobs. The larger the organization, the higher the chance there will be of employees making mistakes regarding the new CCPA requirements without sufficient training.

For most companies, this will mean doing more than broadcasting a 20-page deck to the whole workforce and requiring them to read it. Because of the heightened penalties allowed by CCPA, businesses will want to consider deploying one of the more robust change-management programs they've undertaken in recent years. This will typically involve training modules customized for each corporate function and line of business, and a rolling campaign of communications and advisory assistance right up and through the go-live date of January 2020.

Strategic scoping decisions need to be made

California's 39.5 million residents make it the most populous state in the United States, and its \$2.8 trillion nudges out the UK to claim title to the fifth-largest economy in the world. Any US company going national and any non-US company breaking into the American market will inevitably serve California residents and come under the long arm of the CCPA.

This poses a strategic question for these corporations: Do we afford CCPA rights to only Californians, or do we offer them to our entire base of customers, consumers, and employees? Operationally, there will be a tipping point for each corporation where it becomes more cost-effective to offer a single level of service. From a brand and PR perspective, however, that tipping point may come earlier than expected. If CCPA becomes widely understood, consumers and employees in other states may expect to receive these rights.

CCPA also exempts from its coverage the personal data already covered by the Health Insurance Portability and Availability Act, Gramm-Leach-Bliley Act, Driver's Privacy Protection Act, and the Fair Credit Reporting Act. Healthcare-covered entities and financial institutions should not breathe a sigh of relief too quickly, however. An early read of the law by seasoned privacy attorneys has flagged ambiguities that may not be clarified by the State of California until it is directed to do so by the CPPA by January 2020. Companies in this situation will have a second strategic decision to make: rely on the apparent exemption and do minimal remedial work before January 2020, or begin to address CCPA's requirements now, and de-scope initiatives as these carve-outs become clarified.

Outlook

The period between now and January 2020 represents an opportunity for companies to prepare their programs for the future of privacy and security regulation. Between now and then we can expect companies to continue to deploy new technologies such as artificial intelligence and robotics, and for some of them to fumble and land in the privacy headlines. In what is becoming a global cycle of give and take, we can further expect these fumbles to spur European regulator and legislative action, and the subsequent energy to result in a growing number of U.S. states and other countries to enact their own CCPA-like laws. Corporate privacy leaders who seize this unprecedented moment to help set a data-strategy vision for their companies will be returning to work from the 2019 winter holidays to a career with a new horizon.

For more information

Jay Cline

US Privacy Leader

+1 (612) 596 6403

jay.cline@pwc.com

Thank you to the PwC privacy team that contributed to this report: Jocelyn Aqua, Rachel Blumenthal, Brett Croker, Mike Dolphin, Shanna Holako, Arnab Kumar, Alison Kutler, Eric Lybeck, Lindsey Meyers, and Antonio Sweet.