

MAKE ME **DISAPPEAR**

2020 and beyond – How to
comply to the '*new normal*'
in data privacy and retention
with your current technology



platform3solutions.com

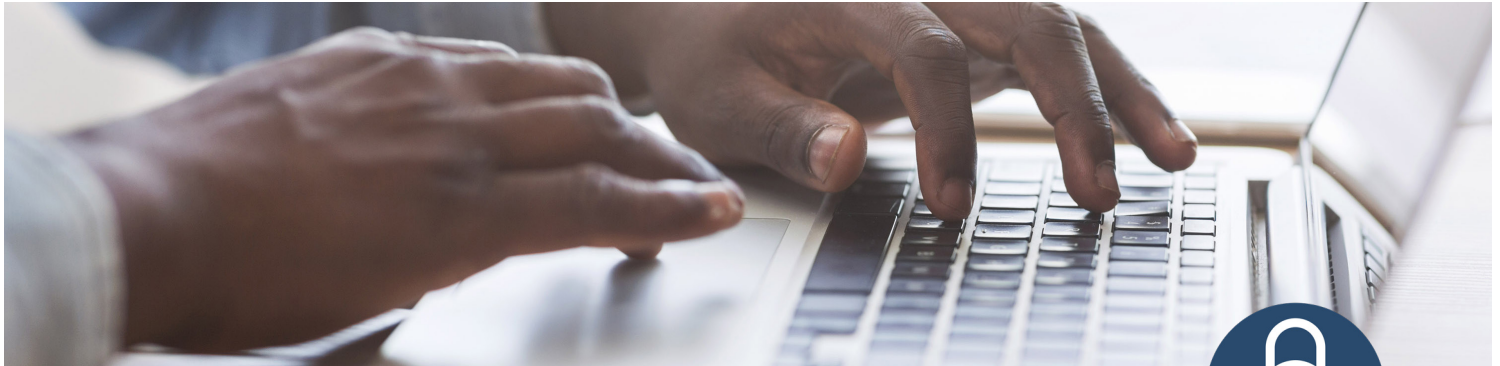
EXECUTIVE SUMMARY

The European law gave companies years to comply while CCPA has given them a few months.

It began with the General Data Protection Regulations (GDPR) law that was enacted in 2018 in the European Union.¹ It has since moved to the United States with the California Consumer Privacy Act (CCPA).² The effect this has on any organization doing business with consumers – rather directly or indirectly - includes:

- The **right to know** what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information;
- The **right to delete** personal information held by businesses and by extension, a business's service provider;
- The **right to opt-out** of sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under the age of 16 must provide opt in consent, with a parent or guardian providing consent for children under 13.
- The **right to non-discrimination** in terms of price or service when a consumer exercises a privacy right under CCPA.³

The European law gave companies years to comply while CCPA has given them a few months.



THE PROBLEM

An economic impact assessment prepared for the California Attorney General's office by an independent research firm found compliance with the regulations will cost businesses between \$467 million and \$16.5 billion between 2020 and 2030. Industry estimates peg initial compliance costs at over \$50 billion.⁴

¹ <https://gdpr.eu/>

² <https://oag.ca.gov/privacy/ccpa>

³ https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

⁴ <https://www.reuters.com/article/us-usa-retail-privacy/do-not-sell-my-info-u-s-retailers-rush-to-comply-with-californias-new-privacy-law-idUSKBN1YYORK>



The California Attorney General told Reuters in an interview that privacy law enforcement will look kindly on those that demonstrate an effort to comply. But they expect plaintiff attorneys to bring lawsuits against a range of businesses that may fail to meet the law's requirements.⁵

But the efforts to truly comply with the essence of the law make for an extensive evaluation of internal databases and information repositories. The more complex the client relationship, the more fragmented the data about clients and the more the customer information resides in unstructured documents and emails – the greater the burden to comply.

Dr. Joe Shepley of Ankura Consulting LLC sums it up best in his article “**5 Information Management Trends of 2020**” – “Check out any survey of C-level executives and corporate boards in the last two years, and privacy is a near-ubiquitous top three concern – and typically it's the primary one. And, beginning with the GDPR, it's been top of mind for regulators as well. In the US, California's CCPA is the best-known example, but at least 10 other states have similar regulations, and at least five proposals for regulation at the federal level are currently being bounced around. All of which is to say that privacy is poised to be top of mind for corporations in 2020 – and will likely continue to be for years to come.”⁶

SANCTIONS & REMEDIES

If proper efforts are not taken, the following sanctions and remedies can be imposed:

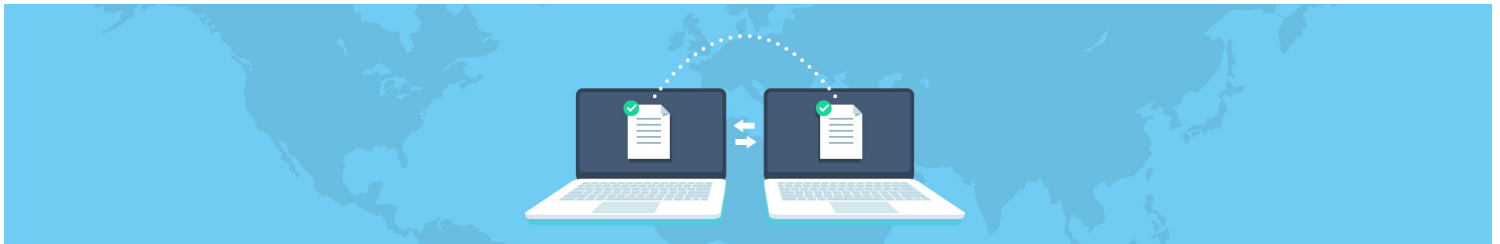
- Companies, activists, associations, and others can be authorized to exercise opt-out rights on behalf of California residents.⁷
- Companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay statutory damages between \$100 to \$750 per California resident and incident, or actual damages, whichever is greater, and any other relief a court deems proper, subject to an option of the California Attorney General's Office to prosecute the company instead of allowing civil suits to be brought against it.⁸

⁵ <https://www.reuters.com/article/us-usa-retail-privacy/do-not-sell-my-info-u-s-retailers-rush-to-comply-with-californias-new-privacy-law-idUSKBN1YY0RK>

⁶ <https://www.cmswire.com/information-management/5-information-management-trends-for-2020/>

⁷ https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

- A fine up to \$7,500 for each intentional violation and \$2,500 for each unintentional violation.⁹
- Privacy notices must be accessible & have alternative format access clearly called out.¹⁰



THE DETAILS

The more complex the relationship with the consumer, the more complex the effort to comply with CCPA. Consider the following:

- **Mergers/Acquisitions** – A company grows through acquisition and have an inconsistent set of databases and definition of customers. Not just in the current online systems, but in anything still running in the data center.
- **Where signatures were needed on documents** – Rather paper or digital - The consumer was required to sign a ‘document’ that defined the length and terms of the relationship. How and where are these documents stored?
- **A migration from old technology to new** – Rather from an older on-premise/homegrown order entry system to a newer cloud environment, many organizations keep the old system running. Not all data is migrated because of the cost, burden or limits placed in the new environment.
- **Legacy systems not up to the task** – Many legacy poses challenges as they were never designed with compliance in mind. Limited of functions, lack of SMEs who know the data, siloed data sets make referential integrity in pinpointing customer’s data a challenge.
- **Inconsistent definition of the customer** – ‘Master data management’ has been a topic for decades and over time, is still not a reality in having a single database standard in defining customers. Multiple customer numbers, misspellings, name changes, address changes – the list goes on. Take this across databases, time and data formats.
- **Referential data integrity is key** – Without a clear understanding of all the relationships, data context, and metadata it is hard to clearly define what makes up the “customer” record.

⁸ https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

⁹ https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

¹⁰ <https://uxdesign.cc/federal-accessibility-laws-dont-matter-california-s-accessibility-laws-do-7367e32755ca>



The requirements placed on organizations as outlined by CCPA imposes new business obligations¹¹:

- Businesses subject to the CCPA must **provide notice** to consumers at or before data collection. Major retailer examples of these changes can be seen at Walmart¹², Target¹³, and Best Buy¹⁴.
- Businesses must **create procedures** to respond to requests from consumers to opt-out, know, and delete. For requests to opt-out, businesses must provide a “Do Not Sell My Info” link on their website or mobile app.
- Businesses must **respond** to requests from consumers to *know*, *delete*, and *opt-out* within specific timeframes. As proposed by the draft regulations, businesses must treat user-enabled privacy settings that signal a consumer’s choice to opt-out as a validly submitted opt-out request.
- Businesses must **verify** the identity of consumers who make requests to know and to delete, whether or not the consumer maintains a password-protected account with the business. As proposed by the draft regulations, if a business is unable to verify a request, it may deny the request, but must comply to the greatest extent it can. For example, it must treat a request to delete as a request to opt-out.
- As proposed by the draft regulations, businesses must **disclose** financial incentives offered in exchange for the retention or sale of a consumer’s personal information and explain how they calculate the value of the personal information. Businesses must also explain how the incentive is permitted under the CCPA.
- As proposed by the draft regulations, businesses must **maintain records** of requests and how they responded for 24 months in order to demonstrate their compliance.

A SOLUTION FOR ACTION

Some steps to take into consideration that help empower this effort:

- **Intake process**
 - Match requestor
 - Verify the requestor
 - Fulfill
- **Have you discovered and mapped** all data sources that have customer data?
- **How do you connect** to the sum of these repositories – no matter the platform or data set.

¹¹ https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

¹² <https://corporate.walmart.com/privacy-security/walmart-privacy-policy/walmart-privacy-policy-frequently-asked-questions>

¹³ <https://www.target.com/c/target-privacy-policy/-/N-4sr7p>

¹⁴ <https://www.bestbuy.com/site/privacy-policy/california-privacy-rights/pcmcat204400050063.c?id=pcmcat204400050063>

- **Build referential integrity** – When you define the “record” or “data topic” making sure you have all the relationships and context before you take action on the data.
- Enrich with **MetaData** to take smart actions, apply business rules and governance.
- **Take action**
 - Defensible deletion and data pruning (make me disappear)
 - Access to PII collected
 - Track and report
- **Governance and compliance must haves**
 - Chain of custody
 - Referential integrity
 - Retention and Disposition
 - Data Lineage
 - Audit



This is where Archon¹⁵, by Platform 3 Solutions, along with their professionals who understand the broad portfolio of legacy systems can help. Archon brings a best practice¹⁶ and immediate result for clients to own and automate their consumer compliance demands.

Call us and learn more about how we can help avoid the high costs of compliance.

¹⁵ <https://platform3solutions.com/products/archon/>

¹⁶ <https://platform3solutions.com/services/>



LEARN MORE

Headquarters

601 Carlson Parkway
Suite 1050
Minnetonka, MN 55305, USA

Phone: (+1) 952 449 5225

Fax: (+1) 612 295 0029

Email: sales@platform3solutions.com

platform3solutions.com
