armanino

PRIVACY UPDATE:
CALIFORNIA CONSUMER PRIVACY ACT

A New Privacy Landscape Emerges

November 2019

TABLE OF CONTENTS

The U.S. consumer data privacy landscape received two separate shocks in 2018, and the shock waves will impact a wide swath of organizations. On May 25, 2018, Europe's sweeping, complex General Data Protection Regulation (GDPR) went into effect, followed on June 28 by the passing of the California Consumer Privacy Act (CCPA). Both these regulations apply to companies in a variety of geographies and across industries. Scrutiny of the way organizations manage consumers' data privacy rights has never been higher, as evidenced by the number of countries and states adopting or considering new data privacy regulations.

The CCPA has an implementation date of January 1, 2020 — but don't let that date lull you into a false sense of complacency. A 12-month look-back provision of the CCPA requires covered entities to provide to consumers a record of the sale or disclosure of their personal information covering the preceding 12 months.

These two pieces of legislation create a privacy environment that is robust and pervasive. The regulators in the European Union (EU) and California — two economic powerhouses — are targeting data collection that pertains to their residents, regardless of the location of the company that collects or processes that data.

The ubiquity of e-commerce today means that companies of any size can easily reach consumers in other states and even internationally — sometimes unintentionally. Now, any business that processes the personal data of California or EU residents must comply with these stringent privacy regulations or face hefty fines. GDPR fines can be as much as 4 percent of global revenue or 20 million euros, whichever is greater. CCPA penalties can be as high as $7,500 per intentional violation. Theoretically, that fine could be levied by treating each record as an individual violation, making the penalties enormous. For large companies that maintain hundreds of thousands of records, these fines could be devastating.

1 OVERVIEW OF THE U.S. PRIVACY LANDSCAPE

For U.S. businesses, these new laws represent a dramatic change in thinking about consumer privacy. U.S. consumer privacy laws have rarely come with strong enforcement provisions or penalties. In contrast, Europe enshrined privacy as a fundamental human right many decades ago. Generally, state and federal legislators in the U.S. have been willing to sit on the sidelines, effectively placing business interests and the widespread use of data ahead of individuals' privacy rights. We are now seeing the beginning of a sea change.

When it comes to business-to-business (B2B) agreements, the topics of privacy and data protection are not new. Contracts and other business agreements regularly address issues such as how to deal with sensitive and proprietary information, who it belongs to, how it can be used, who it can be shared with, who is responsible for protecting it and when it must be returned or destroyed. In contrast, business-to-customer (B2C) commitments have often included privacy terms, but there have been limited avenues for end users to enforce them or hold businesses accountable.

Both the GDPR and the CCPA address these issues in the context of personal information.

The GDPR is a complex regulation, and it applies to any information combined with another piece of information that can be used to identify a natural person. The law applies to data controllers and processors, whether they are operating in the EU or not, so long as the information is about an EU citizen and is collected in relation to the offering of a good or service, or the monitoring of the citizen's behavior.

The CCPA has been rightly described as the strictest privacy bill in the history of the U.S., which is why some call it "GDPR for California." The law covers not only standard personal information, but also information collected by devices, records of internet activity, and household data such as water consumption. It even covers audio, electronic, visual, thermal and olfactory information.

The law applies to any for-profit company that collects personal data from California residents, as long as the business does **any** of the following:

- Generates at least $25 million in annual revenue
- Processes or possesses the personal data of at least 50,000 California residents annually
- Collects at least 50 percent of its revenue from the sale of personal information

Like the GDPR, the California law gives consumers certain rights, including the *right to access* and the *right to erasure.*

The right to access allows consumers to request records on what type of data the organization holds and what is being done with the data. The business must comply in a timely manner, and just as important, it must ensure that the person requesting the information is indeed the consumer in question.

The right to erasure allows the consumer to request that his or her data be deleted. Consumers also have a right to know if their data is being sold to a third party, and they can object to the sale of that data and even opt out of that sale. Organizations cannot discriminate against a consumer based on the exercise of any of these rights.

There are differences between the two laws. The California law will require an opt-out option in which consumers can choose to tell the company not to share or even save their information, with certain exceptions. The GDPR essentially requires consumers to “opt in,” or consent to the collection of their data in the first place.

The rights conferred to Californians and EU citizens are not absolute. There are many exceptions that must be considered. While organizations should act to comply and avoid penalties, they should also consult experts to ensure compliance dollars and human capital are applied in a focused way.

2 UNDERSTANDING THE KEY TERMINOLOGY

It wouldn't be full employment for attorneys, accountants and consultants if there wasn't a host of new terms and distinctions to remember.

First, and perhaps most important, is the "data" or "information" covered by both the CCPA and the GDPR. **In the U.S.** we use the terms **personally identifiable information** (PII) and **protected health information** (PHI/ePHI). PII is any one piece of information that can be used alone, or in combination with other information, to identify an individual natural person. PHI is a specific set of PII that — by the Department of Health and Human Services definition — consists of 18 categories of information, some of them specific to medical diagnosis. **In Europe**, and in the GDPR, the same concept is given the name **personal data.** Finally, **in the CCPA**, the California Legislature used the term **personal information.** While these terms should be used carefully, they are, for most intents and purposes, the same concept.

KEY TERMS AND DEFINITIONS

General Data Protection Regulation	California Consumer Privacy Act
Data subject: An identified or identifiable natural person.	**Consumer:** A natural person who is a California resident, however identified, including by any unique identifier.
Data controller: An individual or organization that, alone or with others, controls the contents and use of personal data. Data processor: An individual or organization that deals with personal data as instructed by a controller for specific purposes, and offers services to the controller that involve personal **data processing.**	**Business:** A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information.
Data processor: An individual or organization that deals with personal data as instructed by a controller for specific purposes, and offers services to the controller that involve personal data processing.	**Service provider:** A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.
Personal data: Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	**Personal information:** 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.
Online identifiers: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	**Device:** Any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.
Processing: Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means. Examples of such operations include collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.	**Processing:** Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means.
	Third party: A person who is neither of the following: the business that collects personal information from consumers; or a person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract.

8 CONSUMER RIGHTS GRANTED BY THE CCPA

1. RIGHT TO KNOW ALL DATA COLLECTED BY A BUSINESS ON THE CONSUMER

Practice point: For businesses to comply with the CCPA, they must have policies and procedures that allow them to properly respond when a consumer exercises her right. Therefore, data mapping and data inventory are key aspects of a CCPA-compliance privacy program. Additionally, defined customer/consumer communication protocols are a way to standardize your employees' responses to consumers requesting access to their data. Finally, the CCPA requires businesses to implement a proper method of verifying the identity of those requesting access to or deletion of data.

2. RIGHT TO SAY NO TO THE SALE OF CONSUMER INFORMATION

Practice point: The CCPA requires a "do not sell my data" link on the organization's webpage and public-facing privacy policy. These are easy changes to make, and it is easy to spot when changes have not been made to an organization's website. Work with internal or external developers to ensure your webpage and privacy policy are up to date on January 1, 2020.

3. RIGHT TO REQUEST DELETION OF THE CONSUMER'S DATA

Practice point: As noted in the first practice point above, some organizational change is necessary to comply. Whether that means enacting and training key employees on new policies and procedures, or reconsidering the manner in which your organization collects, stores, shares and disposes of consumer data (or doesn't), earnest action is required now.

4. RIGHT TO BE INFORMED OF WHAT CATEGORIES OF DATA THE BUSINESS COLLECTS

Practice point: There are many ways in which this compliance requirement can be turned into a marketing opportunity and even a competitive advantage. Armanino has technology solutions that allow an organization to host a "privacy center" that actively displays this required information, and allows management and automation of consumer requests.

5. RIGHT TO KNOW THE CATEGORIES OF THIRD PARTIES WITH WHOM THE CONSUMER'S DATA IS SHARED

Practice point: In many cases, such sharing with third parties may not be strictly necessary to achieve the organization's objectives or offer the service or product to end customers. Management should consider curtailing such sharing and ask the key question: "Are we OK with our customers knowing where this data goes?"

6. RIGHT TO KNOW THE CATEGORIES OF SOURCES OF INFORMATION FROM WHOM THE CONSUMER'S DATA WAS ACQUIRED

Practice point: Documenting data sources can often be more difficult than one would expect, especially for organizations that enrich consumer profiles by merging data from multiple sources. This is part of the data-mapping exercise and should be undertaken long before the looming deadline.

7. RIGHT TO KNOW THE BUSINESS OR COMMERCIAL PURPOSE OF COLLECTING YOUR INFORMATION

Practice point: Organizations may find this an opportunity to craft a compelling story for consumers — or potentially a public relations problem. In either case, organizations should carefully assess how the data they collect and use connects to the product or service they offer.

8. PRIVATE RIGHT OF ACTION REGARDING DATA BREACHES AND UNAUTHORIZED DISCLOSURE RIGHT

Practice point: Organizations that believe their potential exposure is high should consult experts early. Improper responses to consumers requesting data could exacerbate legal troubles and lead to high legal and reputational costs from defending multiple lawsuits.

4 EXCEPTIONS TO THE CCPA

The CCPA will not restrict a business's ability to do the following:

Comply with federal, state or local laws

Practice point: Organizations must preserve data to demonstrate that they complied with the law, properly authenticated a data subject, responded to them in a timely manner and deleted the data. There must be some audit trail.

Collect, use, retain, sell or disclose consumer information that is deidentified or aggregated

Practice point: Organizations should be cautious about data that can still be combined to identify someone. Device data is covered by the CCPA, so organizations should ensure that the data cannot be readily combined to identify a California citizen or other natural person.

Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California

Practice point: For instance, the e-commerce firms that collected the information from the consumer in question while he or she was outside California.

The CCPA is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the U.S. or California Constitution. Therefore, the law provides that organizations subject to any of the following laws are exempted from the CCPA:

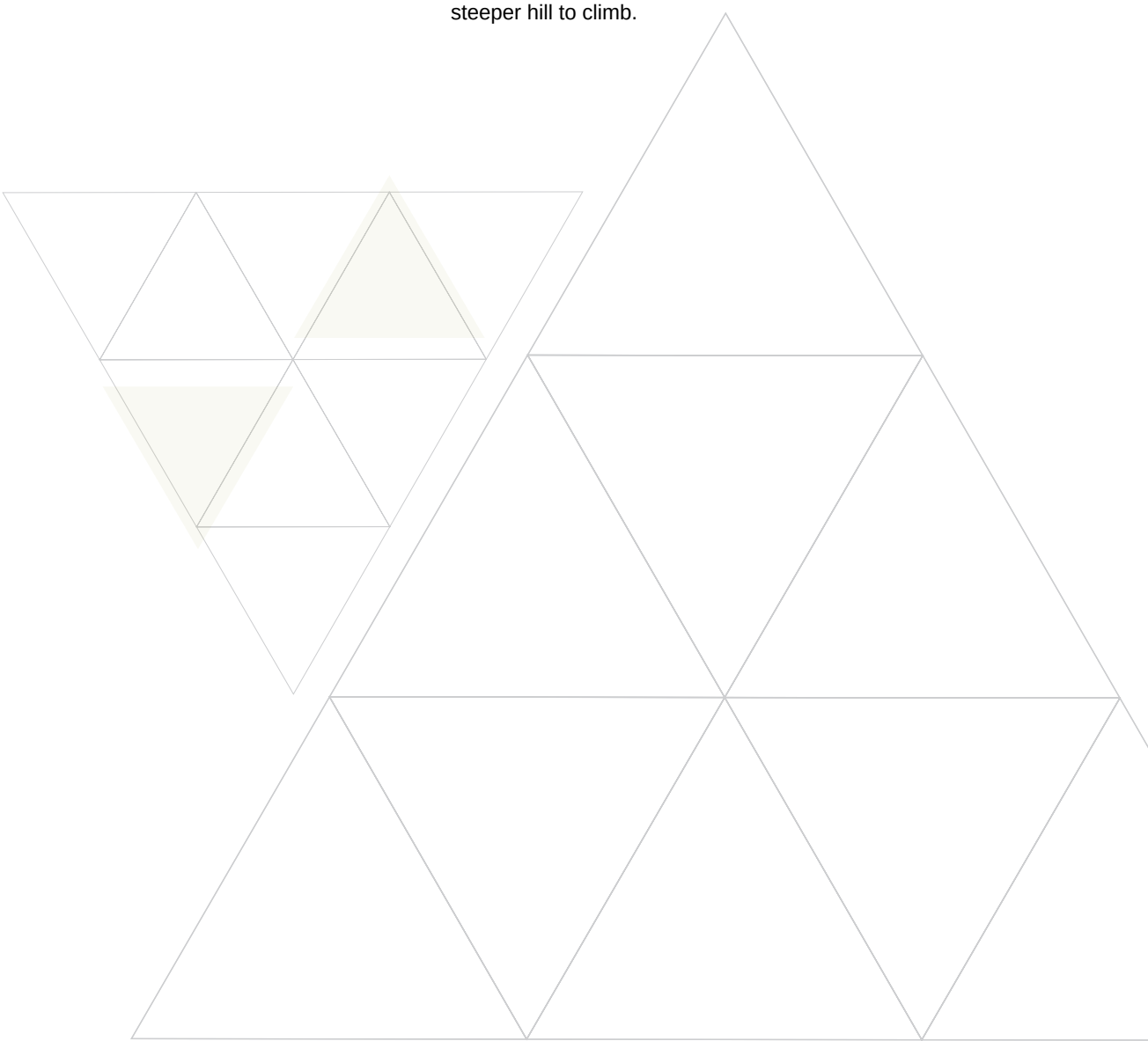
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Gramm-Leach-Bliley Act
- The Driver's Privacy Protection Act
- The California Confidentiality of Medical Information Act
- The Clinical Trials Common Rule

5 COMPARING KEY REQUIREMENTS OF THE GDPR AND THE CCPA

In many respects, the framework of the CCPA is similar to the GDPR. While many businesses took measures to comply with the provisions of the GDPR, it is slightly limited in applicability for U.S.-based businesses that have few EU contacts.

The CCPA will affect a significant percentage of U.S.-based businesses that collect California consumer data in almost any form. However, the CCPA differs from the GDPR in important ways. Overall, the CCPA is far less complex and significantly less stringent than the EU's regulation.

Certain CCPA requirements overlap with the GDPR's individual rights requirements. Generally speaking, organizations that have undertaken efforts to comply with the GDPR will likely have a smooth road to complying with the CCPA. Organizations that are subject to one or both, but have not acted yet, have a steeper hill to climb.



	GDPR	CCPA
Range	Personal data from EU citizens	Personal data from California residents
Right to access	EU citizens have right to access all t heir personal data processed by firms	California residents have right to access their personal data collected in last 12 months, delineated between sold and transferred
Right to portability	Firms have to provide user-friendly interface for exporting and importing certain EU personal data	All access requested must be exported in user-friendly format for California residents, but there is no import requirement
Right to correction	EU citizens have right to correct errors in their data	Not applicable
Right to stop processing	EU citizens have right to withdraw consent	California residents have right to opt out of selling data only
Right to stop automated decision-making	EU citizens have right to require a human to make decisions that have a legal effect	Not applicable
Right to stop third-party transfer	EU citizens have right to withdraw consent for data transfers involving second purposes of special categories of data	California residents have right to opt out of selling data to third parties
Right to erasure	EU citizens have right to erase EU personal data, under certain conditions	California residents have right to erase personal data collected, under certain conditions

6 HOW TO PREPARE

The California law is still in its early days, which makes planning for compliance difficult. Many details are yet to be ironed out by the state's attorney general, who will enforce the rules. The first round of amendments to the law have already been passed, including one change that delayed enforcement six months to July 2020. But given the 12-month look-back provision, covered entities have no time to lose in putting in place systems and processes to track the personal information that they are collecting and disclosing about California residents.

Meanwhile, other regulatory bodies are advancing their own privacy initiatives. The Federal Trade Commission may play a larger role in the privacy landscape going forward. In November 2018, the FTC announced it is seeking comments on privacy and related topics.

Any company subject to the GDPR, the CCPA or any other privacy requirement would be wise to implement data protection and privacy best practices. Data mapping is a great place to start. It involves periodic analysis of what data a company has and how it moves through the organization, as well as who has access to it, how it is shared and how it is married to data collected from other sources.

Beyond compliance with privacy regulations, your larger goal should be to respond to consumer privacy concerns and provide the data protections they expect. One core tenet of data protection is to collect only the information you need. In the realm of "big data," more information has generally been more powerful. More data, more insights; also, more data, more exposure to risk. As the pendulum swings back toward consumer privacy rights, legislators' mindsets are beginning to shift. Following the lead of the GDPR's necessity requirement, more and more states are likely to enact data protection laws requiring organizations to collect only what is necessary to offer a product or service.

The best way to get started is to consult a trusted advisor and expert. Give your Armanino advisor a call to discuss how your organization can protect consumer data, comply with privacy regulations and have meaningful conversations with customers and clients about what your organization is doing to provide data privacy.


Digital Marketing

NOVEMBER 2019

UPDATES TO THE LEGISLATION

A lot has happened recently with the California Consumer Privacy Act that may impact your company's compliance planning and activities. Here are some of the major Fall 2019 legislative updates to be sure you keep in mind.

The CCPA becomes effective January 1, 2020.

New laws amending the CCPA

- **Employment data.** The recent changes to the CCPA do not apply to the collection of personal information from job applicants, employees, business owners, directors, officers, medical staff, or contractors for one year. However, private right of action still applies for breaches of HR data (25).
- **Clarifying amendments & exemptions.** Deidentified or aggregated consumer data are excluded from the definition of personal information and a limited one-year exemption covers certain B2B communications or transactions, and the existing exemption for the federal Fair Credit Reporting Act (FCRA) is broadened (1355).
- **Data brokers.** Requires data brokers to register with the California Attorney General (AB 1202).
- **Data security.** Extends reach of the data covered by California's breach notification and data security statutes in order to expand the CCPA's private right of action for data breaches (AB 1130).
- **Auto industry exemption.** Exempts vehicle information retained or shared for purposes of a warranty or recall-related vehicle repair (AB 1146).
- **Publicly Available Information.** Clarifies the definition of "publicly available" to mean information that is lawfully made available from federal, state, or local government records. Amends the definition of "personal information" to exclude deidentified or aggregate consumer information (AB 874).
- **Disclosure methods.** Toll-free number exemption. Exemption of online-only businesses from the requirement to have a toll-free number for submitting CCPA information and access requests (AB 1564).

Draft regulations under the CCPA

The California Attorney General released the draft regulations under the CCPA to clarify certain unclear provisions of the law and extended new requirements that many businesses may not have included as part of their planning to meet their CCPA obligations (e.g. the rules the readability of privacy notices). While these regulations are likely to be finalized after the CCPA takes effect, they do provide much needed guidance to businesses, particularly, as it involves the handling of consumer requests and options to verify the identity of a requester. The AG is receiving public comments on the draft regulations until December 6, 2019.

The draft regulations address these topics under the CCPA:

1. Notices to consumers
2. Handling consumer requests
3. Verifying consumer requests
4. Special rules regarding minors
5. Nondiscrimination and valuing personal information

UPDATES TO THE LEGISLATION

Detailed requirements for privacy notices: Readability

1. Be easy to read and understandable to an average person
2. Use plain language and avoid technical or legal jargon
3. Use a format that draws the individual's attention to them and makes them readable, including on smaller screens, if applicable
4. Be available in the language that the organization usually contacts the consumer
5. Be accessible to individuals with disabilities

Notice at collection

A business must describe the categories of personal information that it plans to collect from California consumers in a manner that provides meaningful context about what it collects and the category of personal information, including the business or commercial purposes it will be used for.

Presentation

The notice must be given at or before personal information is collected on the homepage for websites, the download page for mobile applications, and in paper notices or signage with a notice URL in the case of offline collection.

When to issue a new notice

New notice must be provided, and explicit consent given by the consumer for a new use or other purposes not explained in the original notice.

Sale of indirectly sourced personal data

A business that does not collect personal information directly from consumers is not required to provide notice at collection to the consumer, but the business cannot sell the PI unless it either:

i) contacts the consumer to provide notice that the business sells personal data and that the consumer has a right to opt-out

ii) obtains a signed attestation from the source confirming that the source gave the consumer the required notice at collection

Notice of right to opt-out of sales

This notice applies only to businesses that sell personal information. Among other things, a business that sells information will need to include a "Do Not Sell My Personal Information" link to a webpage for submitting opt-out requests. A business is exempt from providing a notice of right to opt-out if it:

i) Does not, and will not, sell PI collected during the time period during which the notice of right to opt-out is not posted

ii) States in its privacy policy that it does not and will not sell PI

Note that a consumer whose personal information is collected while a notice of right to opt-out notice is not posted cannot be deemed to have validly submitted a request to opt-out.

UPDATES TO THE LEGISLATION

Notice of financial incentive

This notice is relevant if a business offers a financial incentive to California residents (e.g. a discounted service for use of consumer data). The value of the incentive must be reasonable related to the value of the individual's data, and the business must provide a notice that:

i) Describe the incentive or price/service differences, including what personal data is in question
ii) Instruct consumers how to opt-in, and later opt-out
iii) Explain how the business calculates the value of the consumer data that is used for the financial incentive or the price/service difference

Handling and Verifying Consumer Requests

The CCPA gives new rights to consumers in the state to access copies of their personal information that a business holds and other details about how that information is processed 9right to know), the right to have a business delete certain information (right to delete), and the right to opt out of a business selling their personal information (right to opt out). The AG's released regulations further clarify that the primarily responsibility to give effect to these rights with respect to the personal information held by the business is – the business – and not a service provider. The regulations also detail how businesses should handle consumer requests, including the channels that must be made available to consumers to submit their requests, the SLA for handling received requests, and how businesses should proceed in verifying the identity of a requester.

CCPA intake workflow

Businesses must provide two or more designated methods to submit requests for access to or deletion of personal data, one of which must be a toll-free telephone number. The draft regulations add that at least one designated method must reflect the manner in which the business primarily interacts with the consumer, even if this means more than two methods are used. Note: Certain online-only businesses are exempt from the toll-free number requirement due to a recent amendment.

Submissions Routes

If a consumer submits a request to know or delete through a channel not designated by the business, the business must either accept the request as properly submitted or instruct the consumer how to properly submit the request.

Acknowledgement of receipt

The business must acknowledge receipt of a consumer request within 10 days and provide information about how and when the business will respond.

Responding

- A business can decline to respond with specific data if disclosure would create an unreasonable risk to either the consumer or the business
- A business must not disclose a consumer's social security number, driver's license number or other government identification number, financial account number, health insurance or medical identification number, account password, or account security questions or answers
- If a business denies a request, it must explain the basis of its denial
- In responding to a request to delete, a business need not delete from archived or backup systems (until they actually access or use that system)
- A business must use reasonable security when producing documents

UPDATES TO THE LEGISLATION

CCPA Training

A business must train all personnel who handle consumer requests.

- Record-keeping. A business must maintain records of CCPA requests, and how it responded, for at least 24 months
- Record-keeping for larger businesses. Businesses that annually buys, receives or shares for commercial purposes or sells the personal data of 4 million or more consumers must also compile metrics for each calendar year on the number of each type of consumer requests received and the median number of days within which the business processed it, disclose the metrics in their privacy policy, and establish and implement a CCPA training policy.

Verification

The draft regulations establish certain principles and rules on how businesses must verify the identity of requesters, considering the nature of the request and sensitivity of the personal information involved. For example, the more sensitive the information at issue is, the more the need for a robust verification process. Not much clarity is provided by the draft regulations on how to implement the standards slated for businesses to employ in verifying the identity of requesters. The takeaways:

What is reasonable?

A reasonable method accounts for factors such as:

1. The ability to match identifying information provided by the consumer with personal data held by the business
2. The sensitivity of the PI covered by the request
3. The risk of harm from unauthorized access or deletion
4. The likelihood that requests are made by fraudulent or malicious actors, or are spoofed or fabricated
5. The context of the business's relationship with the customer

Also, applies the data minimization rule. In order to verify a consumer request, a business should match the information in its records with the information provided by the consumer, and avoid requesting additional information from the requester unless needed to verify their identity. The business may use the additional information for verification or fraud-prevention purposes only and must delete this information. Additionally, a business must implement reasonable security to detect fraudulent requests.

Verification should be proportionate to the nature of the request and/or the underlying personal data. For example:

- Requests to know categories of personal data collected must be verified to a "reasonable degree" of certainty (e.g., matching two data points provided by the consumer with those held by the business)
- Requests to know specific personal data collected must be verified to a "reasonably high degree" of certainty (e.g., matching three data points and obtaining a signed identity declaration sworn under penalty of perjury from the requester).
- Requests to delete personal data can be verified to either a reasonable or reasonably high degree of certainty, depending on the sensitivity of the personal data and the risk of harm to the consumer if the deletion were unauthorized.

Agent submitted requests are bound to the procedure adopted by the business to verify the consumer's identity. A business can require written proof from the consumer that the agent is authorized to act on their behalf (with certain power of attorney exceptions).

UPDATES TO THE LEGISLATION

Password-protected accounts

A consumer logging into a password-protected account maintained by the business to exercise a CCPA request is enough to verify the request—unless the business has reason to suspect fraudulent access.

Challenges and reporting obligations

If a business cannot reasonably verify a particular consumer's request, it must respond to the consumer explaining the issue. If a business can never reasonably verify any consumer's request, it must state this in its privacy policy, annually re-evaluate its inability to verify requests, and document its evaluation.

Special rules regarding minors

Minors under 13

A business with actual knowledge that it collects the personal data of minors under 13 must establish and document a "reasonable method" to verify the identity of the minor's parent or guardian who consents to sell the minor's personal data. There are multiple methods to obtain the appropriate consent, such as mailing a consent form signed under penalty of perjury, using a payment card, and having the parent/guardian call or videoconference somebody at the business. The methods must be disclosed in the business's privacy policy. The consent here is separate from the consent required under the Children's Online Privacy Protection Act (COPPA).

Minors ages 13, 14 or 15

A business with actual knowledge that it collects the personal data of 13, 14 or 15-year-olds must establish and document a reasonable process for such minors to opt-in to the sale of their PI. This process must be disclosed in the business's privacy policy.

Closing thoughts...

It is important to note that the AG's regulations are still not finalized, and more changes can come from the public forums that continue to debate all aspects of the regulations until December 6, 2019. While you plan for your company's CCPA obligations, if you have any questions about the legislative developments around the CCPA or any privacy or technology matter, please visit us: Risk Assurance & Advisory Privacy Services.

7 EXPERTS

Liam Collins
Partner-In-Charge,
Risk Assurance & Advisory Services
415.568.3479
Liam.Collins@armaninoLLP.com

Pippa Akem
Senior Manager,
Risk Assurance & Advisory Services
415.568.3473
Pippa.Akem@armaninoLLP.com

STRATEGIC INSIGHT, PRACTICAL ACTION

Armanino[LLP] provides an integrated set of accounting and consulting services to a wide range of organizations — privately held companies, non-profit organizations and public entities — operating in the U.S. and globally. We provide five main areas of service: assurance/audit, tax, consulting, risk assurance and advisory, and business management. Our technology focus and global services are key aspects of our service lines. We work with clients in a large range of industries, including technology, cryptocurrency, manufacturing and distribution, nonprofit, private education, real estate and financial services.

For additional information on GDPR and the California Consumer Privacy Act, contact:
Liam Collins
Partner-In-Charge,
Risk Assurance & Advisory Services
415.568.3479
Liam.Collins@armaninoLLP.com

To learn more about
Armanino's Privacy practice visit:
https://www.armaninollp.com/services/risk-assurance/data-privacy/