California Consumer Privacy Act and General Data Protection Regulation: A Guide to California Businesses

By Foley's Privacy, Security & Information Management Practice

FOLEY

FOLEY & LARDNER LLP

Updated as of December 6, 2019

INTRODUCTION

FOLEY
FOLEY & LARDNER LLP

Beginning with the California Online Privacy Protection Act (CalOPPA) in 2004, California has led the U.S. in adopting laws to protect the privacy of its residents. California continued this trend by enacting the California Consumer Privacy Act of 2018 (CCPA) to become the first state in the U.S. with a comprehensive consumer privacy law. When the CCPA initially becomes effective on January 1, 2020, entities **doing business** in California and their service providers will have new data protection duties and California **consumers** will have new rights regarding their **personal information** (including the right to bring a private action).

Included among these new duties are requirements for businesses to update or create privacy notices, provide consumers a choice whether to permit the selling of their personal information as well as other rights to access or delete their personal information, and create new restrictions on business models that rely on the monetization of personal data. The first section of this guide is designed to help businesses understand the scope of the CCPA as well as identify consumers' rights and highlight obligations for businesses under the CCPA.

Notably, as sweeping as CCPA is, certain organizations that are subject to federal privacy laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) are excluded from the CCPA's provisions for personal information activities related to their core businesses, though they may still be subject to some of the CCPA's requirements for their employee personal information.

CCPA DEFINITIONS

"DOING BUSINESS"

"Doing Business" is not precisely defined in the CCPA. According to the California Franchise Tax Board (FTB Pub. 1060), an entity is considered to be "doing business in California" if it meets any of the following criteria:

- It is actively engaging in any transaction for the purpose of financial gain or profit
- It is organized or commercially domiciled in California, i.e., California is the principal place from which trade or business is directed or managed
- Its California sales exceed an annually adjusted threshold amount or 25% of the entity's total sales
- Its California property exceeds an annually adjusted threshold amount or 25% of the entity's total property
- Its California compensation exceeds an annually adjusted threshold amount or 25% of the entity's total compensation paid by the business

"CONSUMER"

A "Consumer" is a natural person who is a resident of California, i.e., one who is either (a) in California for other than a temporary or transitory purpose or (b) domiciled in California and is outside of California for a temporary or transitory purpose. Californians are therefore not only protected in their roles as consumers (individuals who buy a business's products and services), but also as employees, patients, tenants, students, parents, children, etc.

"PERSONAL INFORMATION"

CCPA greatly expands the definition of Personal Information to any information that relates to, describes, is capable of being associated with, or could reasonably be linked to a particular consumer or household. It includes:

- Real name, alias, or postal address
- Email address, IP address, browsing history, search history, or interaction with a website, application, or advertisement
- Commercial information such as records of personal property, products, or services purchased or considered, or other purchasing and consuming history
- Geolocation data
- Social Security number, driver's license number, or passport number
- Professional or employment-related information

The CCPA's sweeping scope mimics another important international privacy law. The General Data Protection Regulation (GDPR) went into effect on May 25, 2018, repealing the previous Data Protection Directive of 1995. For businesses subject to the GDPR, which includes both businesses that have establishments in the European Union (EU) and businesses outside of the EU that offer their goods and services to individuals in the EU, the GDPR created significant additional privacy obligations as well as new rights for **data subjects.**

The GDPR's obligations include requirements to adopt a Data Protection Officer (DPO) and a representative in the EU for businesses without an establishment in the EU, as well as duties to conduct privacy impact assessments and adopt the principle of privacy by design. Data subjects have the right to obtain information about the collection and use of their personal data as well as a copy of their **personal data,** have their personal data corrected or deleted, and object to and restrict the processing of their personal data. The second section of this guide is designed to help businesses subject to the GDPR understand their obligations and consumers' rights under the GDPR.

Entities that do business in California may be subject to both the GDPR and the CCPA. Although the GDPR and the CCPA have many similarities, compliance with the GDPR is not sufficient to comply with the CCPA. Each of these laws has its own unique requirements. Nevertheless, businesses that have already adopted policies and procedures to become compliant with the GDPR have a significant head start to becoming compliant with the CCPA. The third section of this guide is designed to assist businesses in understanding the differences between the GDPR and the CCPA as well as what they may need to do to become compliant with the CCPA if they are already compliant with the GDPR.

GDPR DEFINITIONS

"DATA SUBJECT"

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 to one or more of the following factors specific to the identity of the data subject:

- Physical
- Physiological
- Genetic
- Mental
- Economic
- Cultural
- Social

"PERSONAL DATA"

Very broad definition meaning any information relating to an identified or identifiable natural person (a "data subject"), including:

- Real name, alias, or postal address
- Email address, IP address, or other online identifiers
- Voice recordings
- Geolocation data
- Social Security number, driver's license number, or passport number
- Professional or employment-related information
- Photographs
- Biometric data

PRACTICAL STEPS FOR PRIVACY COMPLIANCE: HOW FOLEY CAN HELP

FOLEY & LARDNER LLP

Conduct a data map

We help our clients develop data governance programs by determining what type of data is processed, where it is stored, from whom it is received, to whom it is disclosed and for what purposes (e.g., is the data sold?), and for how long it is maintained. This is the fundamental first step an organization should take to determine how it must comply with applicable laws and how to best protect its data. We help clients scale their data mapping exercises to practically meet their business needs.

Update your privacy notice

We handle privacy notice issues for clients — all day, every day — and understand how regulators and litigators view privacy notices. We can review and draft a privacy notice as well as fix inconsistencies, errors, and vagueness to comply with CCPA, GDPR, and other laws, regulations, and guidance.

Draft a playbook to handle consumer rights requests

We help organizations draft and implement internal protocols for handling all types of consumer data requests. For example, we help our clients prepare for data subject access requests, including drafting form response letters and related workflows. We also help clients comply with data subject deletion requests, including handling related data retention issues and contract termination requirements.

Review consent requirements and methodologies

We help organizations comply with consent requirements throughout the world, including those under GDPR and CCPA, as well as the verifiable parental consent requirements of the Children's Online Privacy Protection Act (COPPA).

Update your privacy and security policies and procedures

We review and draft information privacy and security policies and procedures for compliance with applicable laws, preferred privacy and security frameworks, industry best practices, and potential red flags for litigators, courts, or regulators.

Update and negotiate your vendor agreements

We regularly review and draft vendor agreements for required contractual clauses and best practices, including clauses related to privacy, security, and processing of data. We have a deep understanding of what should practically be included in these vendor agreements — from legal requirements to recommended business terms — as a result of decades of handling technology contracts as well as data privacy and security issues for our clients.

Conduct a privacy impact assessment

We help organizations conduct privacy impact assessments to evaluate high-risk data processing activities and determine when consent or opt-out is necessary under applicable privacy laws.

Review, update, and practice your incident response plan

We frequently draft incident response plans and assist with data breach response, including hiring forensic teams and others under attorney-client privilege for the investigation and remediation of a security incident as well as drafting all required breach notifications to individuals, regulators, and credit reporting agencies pursuant to applicable laws. We also regularly conduct tabletop exercises to help our clients prepare for a data breach and handle the response in accordance with applicable laws, industry best practices, and standards.

Review cyber insurance coverages and panel requirements

We evaluate whether organizations have adequate coverage and make recommendations on how to effectively share their business risk with both insurers and vendors. Additionally, we determine whether organizations have panel requirements and make recommendations on how to get their preferred forensic, legal, and communications teams covered under their insurance.

Handle related litigation and enforcement actions

We represent our clients in a wide variety of data privacy and security litigation matters, from consumer complaints, class actions brought by data subjects, and other claims brought by businesses and third parties to government agency investigations and enforcement actions by regulators and attorneys general. Working at the cutting-edge of class action and privacy law, we help organizations manage the civil litigation as well as navigate the related public relations landscape.

Oversee security risk assessments and review resulting risk mitigation plans

We often hire IT firms under attorney-client privilege to conduct risk assessments based on various security frameworks such as ISO/IEC 27001, NIST, CIS, COBIT, and HITRUST. We also help clients determine reasonable security measures in accordance with applicable laws and guidance as well as how to mitigate and address known risks and vulnerabilities in risk mitigation plans.

Conduct privacy and security trainings

We have model materials for training workforce members on how to comply with applicable data privacy and security laws and how to be the organization's front-line defense by protecting against phishing and other cyber attacks. We also regularly conduct Board of Director trainings and assist clients with developing privacy and security benchmarks as well as enterprise-wide risk management tools.

ABOUT FOLEY'S PRIVACY, SECURITY & INFORMATION MANAGEMENT PRACTICE

FOLEY
FOLEY & LARDNER LLP

Foley is not new to data privacy and information security — our lawyers have been advising clients in the space and litigating privacy and security cases for nearly two decades, both addressing the evolution of security and related technology issues as well as identifying creative solutions for managing them and handling related litigation claims throughout that time. Our team regularly conducts privacy and security audits and assessments, including developing and implementing data privacy and information security policies, incident response plans, and vendor due diligence programs. We also provide counseling on FTC compliance, including disclosure and safeguards for online, mobile, and social media information collection, use, and sharing practices; consumer protection and marketing regulations such as CAN-SPAM and the Telephone Consumer Protection Act; and state data security and breach notification laws.

While our goal is to proactively mitigate the potential for a security incident to the maximum extent possible, should an incident occur, within minutes we can bring to bear a complete complement of lawyers capable of managing the response, notification, and remediation process as well as handling any related litigation or regulatory actions stemming from the incident, including class action defense and multi-district litigation coordination. Throughout all of these efforts on behalf of our clients, we help document and validate that their privacy and security policies are current, that their employees are aware of and are properly trained on them, and that they have appropriate internal enforcement mechanisms in place.

In an effort to keep pace with evolving threats, we constantly review new technologies and their applications, and work to refine our approach to information security and risk mitigation. We are considered thought leaders in this area, having written a leading treatise and law review articles that were cited as authority by a number of circuit courts. Additionally, we have testified before Congress on data security issues and served as leaders of privacy and security committees for national organizations.

Our broad depth of knowledge and experience is underscored by the fact that our lawyers carry many of the same industry-recognized and valued professional certifications as auditors and security consultants operating in the space. This exceptional credentialing allows us to assess privacy and security practices not only from a legal perspective, but also from audit and pure information security perspectives.

Our Value

Foley's Privacy, Security & Information Management Practice delivers:

- A holistic approach to data privacy and information security from a team that is credentialed in the space and has been working on privacy and security issues for decades
- An integrated team with diverse industry experience to help navigate the challenging privacy and security landscape
- Layered protection programs that incorporate the latest transactional, investigative, and litigation trends learned from years of practice across multiple industries
- Proactive assessments and management of a client's risk environment
- Tailored programs and integration of compliance frameworks based on a client's unique data environment
- Cost-effective solutions utilizing our best practice policies and work product
- Protection of critical communications between a client's business team, Foley lawyers, and forensic security consultants
- Protection of a client's critical business information, financial data, intellectual property assets, and organizational reputation

To learn more about Foley's Privacy, Security & Information Management Practice, visit www.foley.com or connect with any of the key contacts listed on page 24.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

FOLEY
FOLEY & LARDNER LLP

Scope

The CCPA applies to for-profit organizations that meet **any one of the below criteria** while doing business in California, collecting consumers' personal information, and determining the purposes and means of processing that data:

50,000

Personal information of 50,000 or more California consumers, households, or devices per year

$25 million

Annual gross revenues in excess of $25 million (worldwide)

50% or more

50% or more of annual revenues derived from selling California consumers' personal information

Exemptions

The CCPA completely exempts the following types of **organizations:**

- **Nonprofit organizations:** Nonprofit organizations not receiving profit or financial benefits.
- **Healthcare organizations:** Providers of health care governed by the Confidentiality of Medical Information Act (CMIA) or a covered entity governed by the privacy, security, and breach notification rules under HIPAA, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information.

The CCPA also does not apply to the following types of **information:**

- **Healthcare information:** Medical information governed by the CMIA or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules under HIPAA.
- **Clinical trial information:** Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the U.S. Food and Drug Administration.
- **Publicly available information:** Information that is lawfully made available from federal, state, or local government records.

The CCPA also does not apply to the following types of **activities:**

- **Consumer credit reporting activities:** Activities involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency that provides information for use in a consumer report (as defined in the Fair Credit Reporting Act (FCRA)), and by a user of such a consumer report to the extent governed by the FCRA.

The following types of **information are partially excluded** from the CCPA (however, organizations may still be subject to the obligations of the CCPA for their activities related to other types of data):

- **Information gathered by a state's department of motor vehicles:** Personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994. Businesses are still subject to the private right of action for a failure to reasonably protect employment data that results in a data breach.
- **Vehicle ownership data:** The restriction on a "sale" of personal data does not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to U.S. laws, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.
- **Financial data:** Personal information collected, processed, sold, or disclosed pursuant to GLBA and its implementing regulations or to the California Financial Information Privacy Act.
- **Employment data (until January 1, 2021):** Data collected by a business about a natural person acting as a job applicant to, employee of, owner of, director of, medical staff member of, or contractor of that business as long as it is collected and used solely within the context of that individual's role. Also exempts the emergency contact person of such individuals as well as information that is necessary for the business to administer benefits for a third person related to those individuals. Businesses must still comply with the privacy notice obligations and remain subject to the private right of action for a failure to reasonably protect employment data that results in a data breach.
- **Business-to-business data (until January 1, 2021):** Data reflecting a communication or transaction between a business and an individual acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency within the context of the business conducting due diligence regarding, or providing or receiving, a product or service. Organizations must still comply with the individual's right to opt out of a sale of this information.

High-Level Requirements

The CCPA imposes a number of new data protection duties on businesses and affords consumers with new rights regarding how businesses collect and use personal data:

Implement appropriate security measures. Businesses in California have long been required to implement "reasonable" security measures under Cal. Civ. Code 1798.81.5. The CCPA now holds businesses liable (along with liability for potential statutory damages) in the event of a personal data breach that results from a failure to adopt reasonable security measures.

Privacy notice requirements. The CCPA requires that businesses provide new categories of information in their privacy notices, including information about what categories of personal information are collected, the purpose that such information is collected for, where it is collected from, and to what categories of third parties it is disclosed or sold to.

Consumer right to access data. Consumers have a right to request access to the personal information a business may have on them, including all of the information required in the privacy notice as well as the specific pieces of personal information that the business has collected, in a portable format.

Consumer right to erasure. Within certain limits, consumers have the right to request that their personal information collected or processed by the business be deleted.

Consumer right to opt out of the sale of personal information. The CCPA provides consumers the right to opt out of the sale of their personal information to third parties. This broad definition extends well past the tradition definition of "sale" and extends to the disclosure of personal information for financial or other valuable consideration. However, a "sale" does not occur if the agreement between the business and the vendor contains certain contractual restrictions.

Prohibition on discriminating against consumers who exercise their rights under CCPA. Businesses are not allowed to treat a consumer differently because the consumer exercised a right under the CCPA. However, businesses can offer different prices or services if reasonably related to the value of the consumer's data.

Contractual requirements with service providers. The transfer of information to vendors will not be considered a "sale" under the CCPA if the contract prohibits the vendor from using the personal information for any purposes other than providing the services to the business. Businesses may also consider including minimum security requirements and obligations to assist in consumers' rights to access, delete, and opt out of the sale of their information.

Consumers provided with a private right of action. The CCPA provides consumers with a private right of action, including significant statutory damages, when a data breach occurs as a result of a failure to adopt reasonable security measures.

What Organizations Must Do

Low Impact

- Review and revise existing privacy notices to comply with new requirements
- Review agreements with service providers for CCPA-required contractual clauses

Medium Impact

- Review policies and practices for any discrimination against consumers who exercise their rights under CCPA, including denying goods or services, charging different prices or rates, imposing penalties, providing a different level or quality of goods or services, or suggesting that the consumer will receive any of these for exercising their rights
- Immediately and on an annual basis, review and revise the organization's security policies and procedures, considering security requirements for new types of personal information, and draft or revise a written information security policy; consider conforming risk assessments and security policies and procedures to known industry standards such as NIST

High Impact

- Conduct a data mapping exercise to determine the scope of personal data collection and use given CCPA's broad definition
- Develop procedures for submitting consumer right to access, right to erasure, and right to opt out requests, including for authenticating individuals making requests; develop a "playbook" for handling such access requests and train employees accordingly
- Implement opt-in and parental consent requirements for children under 16 years of age
- Implement technical capabilities to process consumer requests within the required deadlines
- Conduct periodic (annual) risk assessments to determine primary risks to all personal information (including all types of information included in the new definition); consider industry standard audits such as SSAE18 (SOC) or ISO/IEC 27001

Overall Impact to Business

Litigation Issues

Perhaps the most significant impact of the CCPA is the creation of a private right of action for consumers who believe subject business entities have violated the statute's provisions. This private right of action sets forth the provision of statutory damages including the assessment of $100 to $750 per incident, actual damages, and injunctive relief. The ability of consumers to bring litigation to enforce the CCPA presents business entities subject to the statute with the real prospect of facing costly litigation (mostly likely in the form of class action claims) as well as potentially significant liability exposure for a variety of claims such as negligence and unfair business practices. Such actions will focus on the business's efforts to comply with the statute as well as its representations regarding what it does with consumer data and how it protects that data. It is therefore imperative for subject business entities to not only understand CCPA, but also ensure they are compliant with its provisions

Like the GDPR, we expect data subject access requests and claims of violation to begin almost immediately upon the CCPA taking effect on January 1, 2020.

A 30-day cure period is limited to violations that can be cured.

Whether an organization has used "reasonable" security measures may be left to the discretion of a judge or jury under claims for negligence and unfair business practices.

The potential for litigation exists not only for how an organization uses data,but also if it fails to maintain it properly — concerned with unauthorized access, exfiltration, theft, or disclosure. A showing of harm may not be required and a company's representations regarding how it handles data will be closely examined.

The California Attorney General can combine the CCPA with other statutes to potentially extend liability timelines (e.g., California Bus. & Prof. C. §17200, which has a four-year statute of limitations). This cannot be used to create a private right of action for breaches of the CCPA.

The California State Attorney General will issue additional regulations, which may increase potential liability and grounds for litigation.

Risks of Non-Compliance

Regulatory Fines: Up to $7,500 per violation for a failure to adopt reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure

Private Right of Action: Statutory damages between $100 and $750 per consumer per incident or actual damages, whichever is greater

Court Awarded Damages: The Court has broad discretion to grant actual damages, injunctions, declaratory relief, and/or other relief that the Court deems proper, though it *must* consider relevant circumstances, including the nature and seriousness of the violation, number of violations, length of violation, willfulness, and the organization's assets, liabilities, and net worth

FTC Enforcement Actions: Additional fines, consent decrees, and/or ongoing monitoring costs

Reputational Harm

Other California Privacy Laws That Affect Businesses

The CCPA explicitly states that it is intended to supplement both federal and state laws to the extent permitted. As such, it is one of many laws in California that impose obligations on businesses related to how they collect, use, and protect personal information from consumers. To understand the CCPA's scope and requirements and to avoid liability, the CCPA must be read in light of other laws in California, including the following key privacy laws:

- **California Business and Professions Code § 22575:** Requires that operators of commercial websites or other online services that collect personal information post a privacy policy with specific disclosure requirements
- **California Business and Professions Code § 22581:** Requires that operators of an internet website, online service, online application, or mobile application permit minors to remove content or information posted on the website operator's service
- **California Civil Code § 1798.81.5:** Requires that a business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure
- **California Civil Code § 1798.82:** Requires that businesses notify individuals about breaches of personal information with specific required information and, if the breach affects more than 500 California individuals, the State Attorney General
- **California Civil Code § 1798.83:** Requires companies to disclose, upon the request of a California resident, what personal information has been shared with third parties as well as the parties with which the information has been shared
- **California Business and Professions Code § 17200:** Prohibits businesses from engaging in unlawful, unfair, or fraudulent business acts or practices. Because it provides for a four-year statute of limitations for violations, it also is often used to extend the statute of limitations for violations of other California laws.

GENERAL DATA PROTECTION REGULATION (GDPR)

FOLEY
FOLEY & LARDNER LLP

Scope

The GDPR applies to all types of organizations, regardless of their location, if they meet **any one of the following criteria:**

Have an establishment in the EU — when processing is performed in the context of that establishment's activities

Offer their goods and services to individuals in the EU — but requires a level of actively offering, not just a drive-by from the EU

Monitor the behavior of individuals in the EU — to the extent the behavior occurs in the EU

High-Level Requirements

Adequate security. Businesses must implement technical and organizational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data.

Privacy and security by design. Businesses must embed privacy and security considerations in every step of the design process for new products and services.

Data Protection Impact Assessment (DPIA). If processing is likely to present a high risk to the data subjects, businesses must conduct and document, with the advice of the Data Protection Officer, an assessment of processing to be performed, including the risks involved in the processing as well as the protections and processes for mitigating the risks. Businesses must consult with the supervisory authority if the DPIA indicates the processing would result in high risk in the absence of measures taken by the controller.

Data Processing Agreements. Businesses must enter into a contract or legal act with certain required obligations by the processor.

Privacy notice requirements. The GDPR requires that controllers provide consumers with certain information regarding the controller's processing of personal data, including the lawful basis for processing, the legitimate interests of the controller (when applicable), and the duration for which the personal data will be kept.

Appointment of a Data Protection Officer and representative in the EU. Most organizations will need to appoint an independent Data Protection Officer who will report to the highest management level and assist the business to monitor compliance with the GDPR, inform and advise the business on its data protection obligations, provide advice regarding DPIAs, and act as the business's point of contact for data subjects and supervisory authorities. Most controllers that have no establishment in the EU will need to appoint a representative in the EU who will be responsible for the controller's processing activities.

Recordkeeping. Business are required to keep certain records of their processing activities, including why personal data was collected, the categories of personal data processed, the recipient of personal data, and any transfers of personal data to a third country.

Data breach notification. The GDPR requires that controllers notify the supervisory authorities within 72 hours of becoming aware of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. Controllers must provide notice to affected data subjects without undue delay when the personal data breach is likely to result in a high risk to the data subjects' rights and freedoms. Processors are required to notify the controller without undue delay after becoming aware of the personal data breach, regardless of the risk of harm.

Restrictions on transborder transfers. Businesses may only transfer personal data to a third country when the level of protection of data subjects guaranteed by the GDPR is not undermined. In a decision by the EU Commission, a third country, territory, or sector can ensure an adequate level of protection through the adoption of approved safeguards such as binding corporate rules and standard data protection clauses (i.e., standard contractual clauses).

Lawful Basis for Processing

	Data subject has given consent for one or more specific purposes
	Necessary for the performance of a contract where the data subject is a party or to take steps towards a data subject's request prior to entering a contract
	Necessary for compliance with a legal obligation
	Necessary in order to protect the vital interests of the data subject
	Necessary for the purpose of the legitimate interests pursued by the controller, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, when the data subject is a child
	Necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller

Data Subject Rights

What Organizations Must Do

Low Impact

- Review and revise existing privacy notices to comply with GDPR content requirements
- Review trans-border data flow and execute standard contractual clauses, or adopt binding corporate rules or Privacy Shield as required
- Appoint a Data Protection Officer if required
- Appoint a representative in the EU if required

Medium Impact

- Review any processing of sensitive personal information
- Review and revise the organization's data retention policy to minimize personal data collection and retain it only for as long as necessary
- Review agreements with service providers for GDPR-required contractual clauses
- Be prepared to demonstrate compliance

High Impact

- Conduct a data mapping exercise to determine the scope of personal data collection and use and ensure there is a lawful basis for all processing
- Conduct periodic (annual) risk assessments to determine primary risks to all personal information (including all types of information included in the new definition); consider industry standard audits such as SSAE18 (SOC) or ISO/IEC 27001
- Immediately and on an annual basis, review and revise the organization's security policies and procedures, considering the nature and scope of personal information, and draft or revise a written information security policy and incident response policy; consider conforming risk assessments and security policies and procedures to known industry standards such as NIST
- Develop policies and procedures for submitting data subject requests and responding to them within the deadlines; develop a "playbook" for handling such access requests and train employees accordingly
- Implement technical capabilities to process consumer requests within the required deadlines
- Review when consent (no bundling) is necessary as well as the organization's existing process for obtaining consent
- Review and revise the organization's incident response procedures for the ability to provide required notices to supervisory authorities and data subjects within the deadlines
- Perform a privacy impact assessment, if required

Overall Impact to Business

Risks of Non-Compliance

Regulatory Fines:
€10M or 2% of worldwide revenue for "minor" violations; €20M or 4% of worldwide revenue for "serious" violations

Penalties and Criminal Sanctions:
EU member states can set their own rules on penalties and criminal sanctions for infringements of GDPR not subject to administrative fines

Private Right of Action:
Data subject has the right to receive compensation from the controller or processor for the damage suffered

Reputational Harm

CCPA VS. GDPR

A Comparison for Organizations That Are Already Compliant or Working Towards Compliance with GDPR

FOLEY

FOLEY & LARDNER LLP

Organizations compliant with GDPR are *not* automatically compliant with CCPA

While these laws have substantial overlap, there are also a number of differences that may impact an organization's business operations

Organizations compliant with GDPR for all personal data will have a significant head start, but will still need additional work to be compliant with both laws

Organizations that complied with GDPR only for data from EU citizens will need to expand their policies and procedures to cover at least California residents (including employees), but should consider expanding them nationwide as more states in the U.S. propose laws similar to CCPA

Scope: Covered Information

CCPA

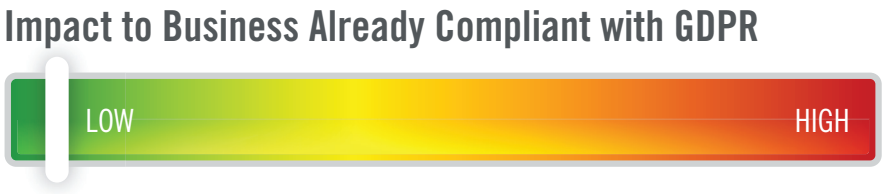
"Personal information" means information that: identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

GDPR

"Personal data" meaning information relating to an identified or identifiable natural person ("data subject").

Comments

- CCPA also allows for information that can be linked with a particular household. Although theoretically broader than GDPR, information linked with a household is also likely linked with an individual in practice.
- CCPA is limited to individuals who are California residents, whereas GDPR only references individuals in the EU, regardless of citizenship or residency.
- There may be some subtle differences between the definitions in extreme cases, but for most organizations, these are essentially equivalent.



Scope: Covered Organizations

CCPA

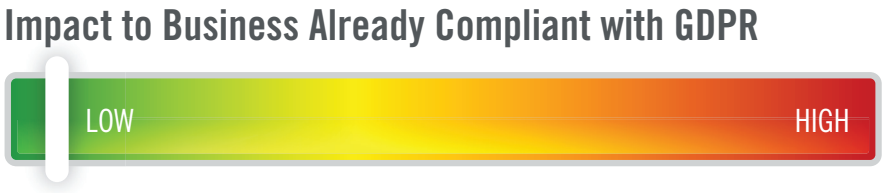
Applies to a for-profit legal entity (or sole proprietorship) collecting personal information about consumers that: (a) either alone or jointly with others, determines the purpose and means of the processing of consumers' personal information; ***and*** (b) does business in the State of California; and ***either*** (i) has annual gross revenue over $25,000,000; (ii) buys, sells, receives, or shares for commercial purposes the personal information of 50,000 or more consumers, devices, or households, on an annual basis; ***or*** (iii) derives 50 percent or more of their annual revenue from selling consumers' personal information.

GDPR

Anyone who, as a controller or processor: (a) processes personal data in the context of an EU establishment (whether or not the processing takes place in the EU); or (b) without having an EU establishment, processes personal data of ***data subjects in the EU*** in relation to offering them goods or services, or monitoring their behavior.

Comments

- CCPA is narrower than GDPR in that most of its obligations directly apply to organizations that would be a "controller" under GDPR. "Service providers" under CCPA are similar to the concept of a "processor" under GPDR, and the categorization of an entity as a "business" or a "service provider" under CCPA is likely to be as challenging as categorizing an organization as a processor or controller under GDPR. The CCPA generally does not include detailed obligations for service providers; however, it does require them to comply with requests for deletion. Service providers are also subject to CCPA's statutory fine structure for their own violations.
- CCPA only applies to organizations that do business in California, whereas GDPR has an extra-jurisdictional reach when processing personal data about a data subject in the EU.
- Organizations are only subject to CCPA if they meet any one of the listed thresholds. GDPR applies to large and small businesses alike if their activities fall within its scope.



Transparency (Privacy Notice) Obligations

CCPA

A specific privacy notice to consumers is required at or before the point of collection and should include: (a) the categories of personal information to be collected; and (b) the purposes for which the categories of personal information will be used.

The privacy notice must be updated at least every 12 months to include: (a) a description of consumers' specific rights under CCPA and methods for consumers to exercise those rights (including a link to "Do Not Sell my Personal Information," if applicable); (b) the categories of personal information collected, sources, and categories of third parties the personal information was shared with over the prior 12 months; and (c) the categories of personal information disclosed or sold (or a statement that the business has not engaged in any such sale or disclosure).

GDPR

The controller must provide a privacy notice to the data subject at the time of collection that contains: (a) the identity and contact details of the controller; (b) any recipients or categories of recipients of the personal data; (c) the legal basis and purposes for the processing; (d) the retention period for the personal data; (e) a description of data subject rights and how to exercise them; (f) information about the controller's representative and Data Protection Officer, if applicable; (g) the intent to export data and protections afforded to exported data; (h) whether the provision of personal data is required by law or in connection with a contract; and (i) any automated decision-making.

Comments

- Most of the information required by CCPA is already required by GDPR.
- CCPA does, however, have some more specific obligations related to personal information that is sold.
- CCPA also requires an update to some disclosures every 12 months, whereas GDPR likely requires it immediately.
- The data subject rights are similar, but the rights and limitations on those rights are not identical.
- Organizations will likely need to update their privacy notices for compliance with CCPA. Organizations may wish to consider California addendums that specifically address residents of California to maintain the principle that the privacy notice remains in clear and concise language. This may also be beneficial as more states consider similar, but differing, laws.

Impact to Business Already Compliant with GDPR

© 2019 Foley & Lardner LLP

Right of Access/Portability

CCPA

Consumers have the right to obtain certain information from businesses regarding the categories of personal information collected, third parties with whom the information is shared, sources of the information, and the purpose for collecting or selling personal information.

GDPR

Data subjects have the right to obtain confirmation from a controller about whether personal data about them is being processed and, if so, the categories of personal data concerned, the recipients or categories of recipient with whom the data is shared, any available information about the source, purposes of processing, the existence of data subject rights, the retention period for the personal data, and any automated decision-making.

Comments

- The rights of access are similar between CCPA and GDPR, although there are some subtle differences in the limitations of the right to access.
- Organizations can largely use the policies and procedures adopted for GDPR with CCPA. However, these policies and procedures should keep in mind the subtle differences in limitations to ensure they are not relying on a GDPR limitation not available under CCPA. In most cases, however, organizations that adopt their GDPR policies for CCPA will provide additional rights to California consumers not required under CCPA.

Impact to Business Already Compliant with GDPR

CCPA

Businesses that receive a verifiable request relating to the above must provide a copy of the information to the consumer within 45 days. The information should be delivered through the consumer's account or, if the consumer does not have an account, in a readily usable and easily transmittable format.

GDPR

Controllers must comply with a request without undue delay and generally within one month of receipt. Data subjects may also receive a copy of their personal data or request that the original controller transmit the personal data directly to another controller.

Comments

- GDPR is broader than CCPA in that it also includes the right to have personal data directly transmitted to another controller — CCPA only requires that the information be provided to the individual in a readily usable format.

Impact to Business Already Compliant with GDPR

Right to Erasure (Right to Be Forgotten)

CCPA

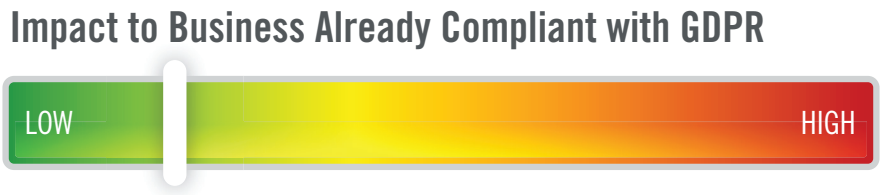
Consumers have the right to request deletion of personal information a business has collected from them.

GDPR

Data subjects have the right to erasure by the controller of personal data about them in certain limited circumstances.

Comments

- Several differences exist between the right to deletion under CCPA and the right to be forgotten under GDPR.
- CCPA only provides a right to have data collected ***from*** the consumer deleted; the right under GDPR extends to all personal data ***about*** a data subject.
- The exceptions under CCPA are broader than the exceptions under GDPR (including when information is needed for internal uses that are aligned with the consumer's expectations).
- Organizations that already comply with GDPR may use the same measures with minor changes; however, this may grant consumers more deletion rights than necessary under CCPA. Broader rights may result in a loss of potential customers. Customers may wish to create California-specific policies to respond to deletion requests.



Right to Opt Out/Choice

CCPA

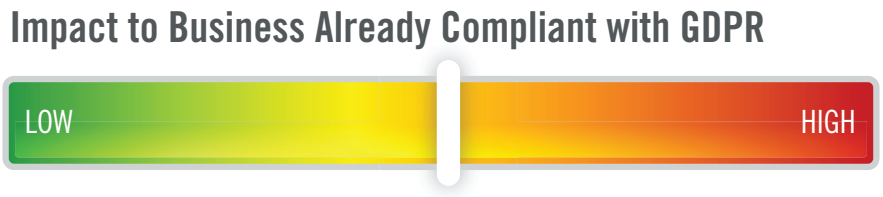
Consumers have the right to opt out of the sale of their personal information. For personal information regarding a child under the age of 16, a business must obtain opt-in consent. If the child is between 13-16 years of age, this may be given by the child itself. Otherwise, the opt-in consent must be provided by a parent or guardian. Organizations must provide a "Do Not Sell My Personal Information" link on applicable websites.

GDPR

GDPR does not explicitly provide an express right for an individual to opt out of the sale of their personal information. However, generally the sale of personal information is not necessary for the performance of the services, which will require the consent of the data subject (which can always be withdrawn). Therefore, the sale of most personal information under GDPR is likely to be as an opt-in.

Comments

- GDPR contains a broader requirement to generally require consent for the sale of personal information (i.e., an opt-in). It also contains a broader right for data subjects to withdraw consent or for data subjects to restrict or object to the processing of their personal information.
- Organizations that already comply with GDPR will largely comply with CCPA, although their method of withdrawing consent will need to comply with the requirements for a link on applicable websites under CCPA. However, businesses that choose to require California consumers to opt in will be greatly restricting their ability to sell personal information (if they do so at all).



KEY CONTRIBUTORS

FOLEY
FOLEY & LARDNER LLP

James R. Kalyvas
Partner and Co-Chair

Los Angeles
jkalyvas@foley.com
213.972.4542
Profile

Eileen R. Ridley
Partner and Co-Chair

San Francisco
eridley@foley.com
415.438.6469
Profile

Chanley T. Howell
Partner

Jacksonville
chowell@foley.com
904.359.8745
Profile

Jennifer L. Rathburn
Partner

Milwaukee
jrathburn@foley.com
414.297.5864
Profile

Aaron K. Tantleff
Partner

Chicago
atantleff@foley.com
312.832.4367
Profile

Jennifer J. Hennessy
Senior Counsel

Madison
jhennessy@foley.com
608.250.7420
Profile

Steven M. Millendorf
Senior Counsel

San Diego
smillendorf@foley.com
858.847.6737
Profile

About Foley

Foley & Lardner LLP looks beyond the law to focus on the constantly evolving demands facing our clients and their industries. With more than 1,100 lawyers in 24 offices across the United States, Mexico, Europe, and Asia, Foley approaches client service by first understanding our clients' priorities, objectives, and challenges. We work hard to understand our clients' issues and forge long-term relationships with them to help achieve successful outcomes and solve their legal issues through practical business advice and cutting-edge legal insight. Our clients view us as trusted business advisors because we understand that great legal service is only valuable if it is relevant, practical and beneficial to their businesses.

FOLEY

FOLEY & LARDNER LLP

AUSTIN | BOSTON | BRUSSELS | CHICAGO | DALLAS | DENVER | DETROIT | HOUSTON | JACKSONVILLE | LOS ANGELES | MADISON | MEXICO CITY | MIAMI
MILWAUKEE | NEW YORK | ORLANDO | SACRAMENTO | SAN DIEGO | SAN FRANCISCO | SILICON VALLEY | TALLAHASSEE | TAMPA | TOKYO | WASHINGTON, D.C.

ATTORNEY ADVERTISEMENT. The contents of this document, current at the date of publication, are for reference purposes only and do not constitute legal advice. Where previous cases are included, prior results do not guarantee a similar outcome. © 2019 Foley & Lardner LLP | 19.MC18783