HBR
CONSULTING

CCPA for Information Governance Professionals

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

Introduction

On January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) will go into effect.[1] Under this law, California consumers have greater rights to know what personal information is collected about them and whether that information is disclosed or sold to third parties. The law provides consumers with the right to stop the disclosure or sale of their personal information.

In addition to these rights, the law gives California consumers the right to request deletion of personal information retained by an organization while remaining eligible for the same service and price received by those consumers who do not request deletion. These two provisions create some of the biggest challenges for information governance professionals, especially those who focus on the records management portion of information governance.

Under this law, California consumers have greater rights to know what personal information is collected about them and whether that information is disclosed or sold to third parties.

Are the CCPA and the European Union's General Data Protection Act the Same?

The CCPA is not the California version of the GDPR. For information governance professionals, it helps to know the distinctions between how the CCPA and the GDPR define "personal data," as well as the differences in "retention requirements" and "staffing requirements."

Definition of Personal Data

The GDPR broadly defines personal data as "[a]ny information relating to an identified or identifiable natural person ('data subject')."[2] This broad definition caused many information governance professionals to question whether the processing of email addresses, business contacts, metadata and any other data that can be traced back to a person is subject to GDPR restrictions.

California provides a more concise definition. The CCPA defines personal data as information "that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." For additional clarification, the law then provides examples such as addresses (IP, email and physical), biometric data, employment information, internet activity and unique identifiers (account numbers, social security numbers).[3]

The CCPA is not the California version of the GDPR.

The California law further refines the definition in two ways. First, the law is limited to "consumer information." This means business contacts and other information not associated with consumers are not subject to CCPA requirements. Second, the California law takes note that "publicly available information" is not considered personal information. Publicly available information is information available from federal, state or local government records.[4]

Retention of Personal Data

Under the GDPR, the retention ("processing") of personal data is limited to information retained by consent, contract, legal requirement, vital interests, public interests or legitimate interests.[5] As a result, under the GDPR, if an organization retains personal data, that organization must be able to justify the retention reason based on these requirements and retain the information for "no longer than is necessary for the purposes for which the personal data are processed."[6]

The CCPA does not limit the right of an organization to retain personal data. So long as the subject has not objected, organizations may retain personal information without the need to justify their purpose. If a California person has contacted an organization and requested the deletion of their personal data from the organization's systems, the organization must respond within 45 days and delete that personal information if there is no other legal reason to retain that information.[7]

Staffing Requirements

The GDPR requires organizations to have a specific staff member responsible for the lawful processing of personal data. This person is referred to as the data protection officer.[8] The data protection officer may be a designated person within the organization or a person designated through a service contract. Under the CCPA, an organization is not required to designate a person responsible for CCPA compliance.

The CCPA does not limit the right of an organization to retain personal data. So long as the subject has not objected, organizations may retain personal information without the need to justify their purpose.

Who Is Subject to CCPA Requirements?

The CCPA does not apply to every organization. The CCPA is designed to protect California residents.[9] To accomplish this, the law is limited to for-profit businesses with annual gross revenues in excess of $25 million that sell or share for commercial purposes the personal information of 50,000 or more consumers and/or derive 50 percent or more of their annual revenues from selling consumers' personal information.[10] This definition means that government agencies, non-profit organizations and

small companies not involved with the selling of personal information are not subject to the CCPA. The CCPA also provides an exception for medical information covered by other laws, such as the Confidentiality of Medical Information Act and HIPAA.[11] In those cases, organizations should continue to comply with policies consistent with the requirements under those laws. Therefore, to determine whether your organization is subject to the CCPA ask the following questions:

- Are you a for-profit organization?
- Do you do business in California (or with California residents)?
- Do you have gross revenues exceeding $25 million or collect or sell large amounts of personal data?

If your organization answers "yes" to the questions above and does not fall within the limited scope of exceptions, then your organization is subject to the CCPA.

What Are the Primary Responsibilities Under the CCPA for Information Governance Professionals?

Organizations subject to the CCPA must be able to respond to consumer requests related to the retention and use of their personal data. This means that, upon request of the consumer, organizations must comply with the following requirements within 45 days:

- Disclose free of charge the categories and specific pieces of personal information on that person the business has collected or sold over the past twelve months (the twelve-month period is referred to as the "look-back" period);[12]
- Delete any personal information about the consumer that the business has collected from the consumer or respond with a reason why the information cannot be deleted;[13]
- Direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information (this right may be referred to as the right to opt out);[14] and
- Deliver the same services as are received by those who have not exercised their rights under this law, i.e., not denying services, charging a higher price or providing a different quality.[15]

If a consumer does make a request for deletion of personal data, organizations should not immediately delete the information. Instead, the organization should determine if the information (1) is needed to complete a transaction with that consumer; (2) is needed to detect illegal activity by the consumer; (3) is associated with the exercise of free speech; (4) is necessary for research and the consumer previously provided informed consent; or (5) is required by law or regulation for continued retention. If it is determined that the information cannot be deleted upon request based on the above reasons, the organization must still respond to the request within 45 days with an explanation.

> Organizations subject to the CCPA must be able to respond to consumer requests related to the retention and use of their personal data. This means that, upon request of the consumer, organizations must comply with requirements within 45 days.

How Should Information Governance Professionals Prepare for the CCPA?

Information governance professionals play a vital role in CCPA compliance. To ensure compliance, information governance professionals should prepare to take the following actions:

- Determine whether their organization is within the scope of the CCPA. This law is designed to protect California consumers. As a result, it has a limited scope.
- Locate consumer personal data retained by your organization. Your organization may have multiple systems that contain personal data. As an information governance professional, you should be able to identify all systems with consumer data.
- Identify the reason for retaining personal data. Consumer data is retained for a variety of reasons, including legal or contractual obligations, the need to provide services to that consumer or marketing.
- Respond to consumer data requests. If a consumer makes a verifiable request for information or action on their personal data, organizations have 45 days to properly respond. Failure to respond will trigger actions by the State of California.
- Act upon consumer requests. If an organization determines there is no legitimate reason to retain the information and a consumer has requested deletion of that information, the organization must have a process in place to ensure the information is deleted. If there is a legitimate reason to retain the information, then the organization must be able to identify that reason and properly respond to the consumer with an explanation.

Conclusion

The CCPA, along with the GDPR and other data protection laws, is yet another signal that the “keep everything forever” culture will not work. Consumers and law makers are pushing back. In some ways, personal information belongs to that individual, and organizations are merely the custodian and caretakers of that information. Companies must take responsibility and care of that information. For these reasons, information governance professionals must play an even stronger role in ensuring that

records are maintained for the appropriate amount of time and in the right location. When organizations retain consumer personal information in many systems, with no rule or limitations and with multiple copies floating around, the organization is not being a good caretaker. But proper information governance that includes custody control, appropriate retention and reasonable access will result in minimal risk to your organization, as well as satisfied consumers.

Connect With Our Experts

For further assistance on the CCPA and other information governance issues, please contact:

Laurie Fischer
Managing Director

O 312.638.5127
E LFischer@hbrconsulting.com

Tom Corey
Senior Manager

O 312.638.5125
E TCorey@hbrconsulting.com

Sources

[1] California Consumer Privacy Act (CCPA), Cal. Civ. Code 1798.198
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

[2] General Data Protection Regulation (EU) 2016/679, Art. 4
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679)

[3] Cal. Civ. Code 1798.140(o)(1)

[4] Cal. Civ. Code 1798.140(o)(1)(K)(2)

[5] Reg. (EU) 2016/679, Art. 6

[6] Reg. (EU) 2016/679, Art. 5(1)(e)

[7] Cal. Civ. Code 1798.105 and 130

[8] Reg. (EU) 2016/679, Art. 37

[9] Cal. Civ. Code 1798.140(g)

[10] Cal. Civ. Code 1798.140(c)

[11] Cal. Civ. Code 1798.145(c)(A)

[12] Cal. Civ. Code 1798.100(a)

[13] Cal. Civ. Code 1798.105(a)

[14] Cal. Civ. Code 1798.120(a)

[15] Cal. Civ. Code 1798.125(a)

[16] Cal. Civ. Code 1798.105(d)

HBR
CONSULTING

HBR Consulting (HBR) delivers advisory, managed services and software solutions that increase productivity and profitability, while mitigating risk for law firms, law departments and corporations. As trusted advisors with deep industry experience, clients partner with HBR to achieve significant, sustainable results.

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

advisory | managed services | software solutions | insights