California Consumer Privacy Act Series: Part 3

Data Privacy Tools: Data Mapping, Legitimate Interest Analysis, and Data Protection Impact Assessments

Prepared by CONEXXUS

Overview

In the previous CCPA Series articles we outlined the rights and requirements of the CCPA and discussed the new privacy processes related to verification and data subject requests. This article discusses three foundational data privacy tools that are available to assist organizations in complying with CCPA and in creating a sustainable privacy program: data mapping, legitimate interest assessments (LIAs), and data privacy impact assessments (DPIAs).

Data Mapping

What is it?

Data mapping is a common data management tool that is used to identify and document data processed by an organization (e.g., within which systems are data found and processed, within which databases are data stored). In terms of the CCPA, a data map of personal data is foundational to inform the creation of a privacy policy, as well as define processes for consumer access and deletion requests. A data map made for other purposes, such as to meet GDPR requirements or during regular data management activities, may not be sufficient for CCPA compliance purposes due to the unique scope CCPA applies to the definition of personal information. While CCPA does not require an organization to keep a data map as part of compliance with the law, it is highly recommended to do so to ensure compliance with other requirements.

How to do it?

Data mapping is conducted through manual effort (interviews, surveys, spreadsheets) or using automated data mapping tools. Structured data that is organized in systems and databases is usually easier to identify and document. By comparison, unstructured data that lives in emails, documents, etc., can be more difficult to locate and summarize when data mapping. As well as capturing the data elements within an organization, one must also consider the source of the data, where it is stored, how it is used and processed, and with whom it is shared. The method of data collection plays a role in defining the scope of the data mapping exercise. How data is collected provides context for determining whether the data qualifies as personal information under the CCPA. Data mapping exercises are needed when data is integrated (e.g., data warehousing), transformed, or migrated.

Why do it?

First and foremost, the CCPA disclosure and privacy policy requirements can only be met if an organization knows about the data it collects. Thus, a data map represents the single organized source to provide all of that information and ensure nothing is missed. Data maps are also critically important for organizations to design processes to respond to data subject access and deletion requests, especially for organizations that want to design technical or automated solutions to these requests. Data mapping exercises provide additional organizational benefits, such as insight into security risks and business inefficiencies.

Legitimate Interest Analysis

What is it?

A Legitimate Interest Analysis ("LIA") serves as "short form" of a DPIA (see below), to determine how its legitimate interests are balanced against the privacy rights of consumers. While the CCPA does not require an organization to perform an LIA as part of compliance with the law, it is a risk mitigation tool.

How to do it?

A LIA should contain a brief analysis of its purpose(s) for collecting and processing personal information, with whom it shares such personal information, and

California Consumer Privacy Act Series: Part 3

Data Privacy Tools: Data Mapping, Legitimate Interest Analysis, and Data Protection Impact Assessments

what risks may be associated with specific actions related to data collection/usage.

Why do it?
An organization may wish to conduct an abbreviated investigation into its privacy actions. It is an easier step for an organization to develop documentation of its reasoning for taking certain actions to present in case of a complaint/ investigation into its compliance.

Data Protection Impact Assessment

What is it?
A Data Protection Impact Assessment (DPIA) is an analysis designed to help identify and minimize the data protection risks of a business, product, or service, including when an organization initiates a new project. A DPIA should be considered for any major project that involves the use of personal data. DPIA can be implemented into a privacy program as templated forms that must be filled out and evaluated during an in-flight project.

How to do it?
Project teams in conjunction with privacy experts should evaluate any impact of privacy requirements on in-flight projects. DPIA should include evaluation of the processing:

- need/nature
- scope
- context
- and purpose

DPIA should identify the risks of the data processing and identify measures to mitigate the risks. This may include requesting information from a third party processor if the project includes a new or existing vendor.

Why do it?
Organizations must continue to evolve and adapt; part of that includes change to their businesses. It is critical that as an organization grows, they continue to evaluate privacy considerations and ensure they remain compliant with relevant privacy laws. GDPR requires a DPIA whenever a type of processing "is likely to result in a high risk to the rights and freedoms of natural persons." CCPA does not explicitly require DPIAs to be performed. However, it is recommended that all privacy teams consider using DPIAs as a tool to identify and mitigate risk.

Conclusion

Data mapping and legitimate interest/data protection impact assessments are important tools used by a privacy team to meet privacy requirements such as the CCPA. Learning how to conduct and implement these tools as part of your privacy program is critical to successful request processing and ongoing compliance efforts.

Conexxus Data Privacy Working Group

The Conexxus Data Privacy Working Group is tasked with creating educational pieces for the convenience and retail fuel industry on existing and future data privacy legislation.

Visit conexxus.org/resources/data-privacy to view the other articles in this CCPA series and additional Data Privacy resources and webinars authored by this working group.

Conexxus members: We encourage you to participate in this working group! Please visit the Data Privacy group page and request to join: (conexxus.org/groups/data-privacy).

Written by the Conexxus Data Privacy Working Group

Sources: California Legislative Information: California Consumer Privacy Act of 2018 SB-1121