CARLTON
FIELDS

An Overview of Data Mapping

Data mapping is a critical first step in privacy and cybersecurity readiness. The process determines what information a business collects and how it uses, stores, and transfers that information, with a focus on personal information and other sensitive information. The business then uses the resulting "map" to assess compliance with applicable privacy laws and contract obligations, prepare for reporting on that data to a consumer or regulator under applicable law, and take operational steps to secure the data. Building a data map is also important to the business's creation of an accurate privacy policy, retention schedule, and associated other internal policies and procedures. Below are some of the key steps in creating a data map.

1. **Data sources.** How does data come into the company? What are the sources for the collection of personal or sensitive data? This could include, for example, point of sale, web or paper forms, information taken from phone calls, and information gathered passively from a potential customer's visit to the business's website.

2. **Data types.** What is the nature of the data that the business collects? This could include personal information such as names, dates of birth, email addresses, and more sensitive personal information such as Social Security numbers, driver's license numbers, or payment card information. Is the information consumer information, or is it information of individuals in their corporate capacity (*e.g.*, the email address of a corporate customer representative)? If the data mapping includes sensitive information other than personal information, such as trade secrets information, this would also be noted.

3. **Data collection purposes.** Why is the business collecting each item of data? That is, is it to process a loan application, for marketing purposes, or both?

4. **Data storage.** Where are the pieces of data stored throughout the business's systems, including local, cloud, and network storage?

5. **Data access.** Who has access to the data within the business's system?

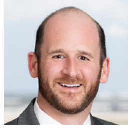
6. **Data usage.** How is the data actually used, and by whom? This information is used to compare whether the usage of the data lines up with the purpose for which it was collected.

7. **Data sharing.** Once the data is collected, who sees it or can see it? Does it ever leave the business? To whom does the data go and for what reason? Is there any sale of the data, such as for money or any other thing of value?

8. **Data timeline, retention, and deletion.** How long is the data retained? Is there automatic or manual deletion and, if so, what are the triggering events? Are like pieces of data deleted in a like manner? How is data deleted, and is the deletion effective?

9. **Data security.** What are the protections around the data? Is there encryption applied to personal and other sensitive information, and does that encryption apply both at rest and in transit?

Contacts



John E. Clabby
jclabby@carltonfields.com
www.carltonfields.com/jclabby
813.229.4229

Patricia M. Carreiro
pcarreiro@carltonfields.com
www.carltonfields.com/pcarreiro
305.539.7314

Joseph W. Swanson
jswanson@carltonfields.com
www.carltonfields.com/jswanson
813.229.4335

Eden Marcu
emarcu@carltonfields.com
www.carltonfields.com/emarcu
813.229.4148

www.carltonfields.com

Atlanta · Hartford · Los Angeles · Miami · New Jersey · New York · Orlando · Tallahassee · Tampa · Washington, D.C. · West Palm Beach

Carlton Fields practices law in California through Carlton Fields, LLP.

January 2023