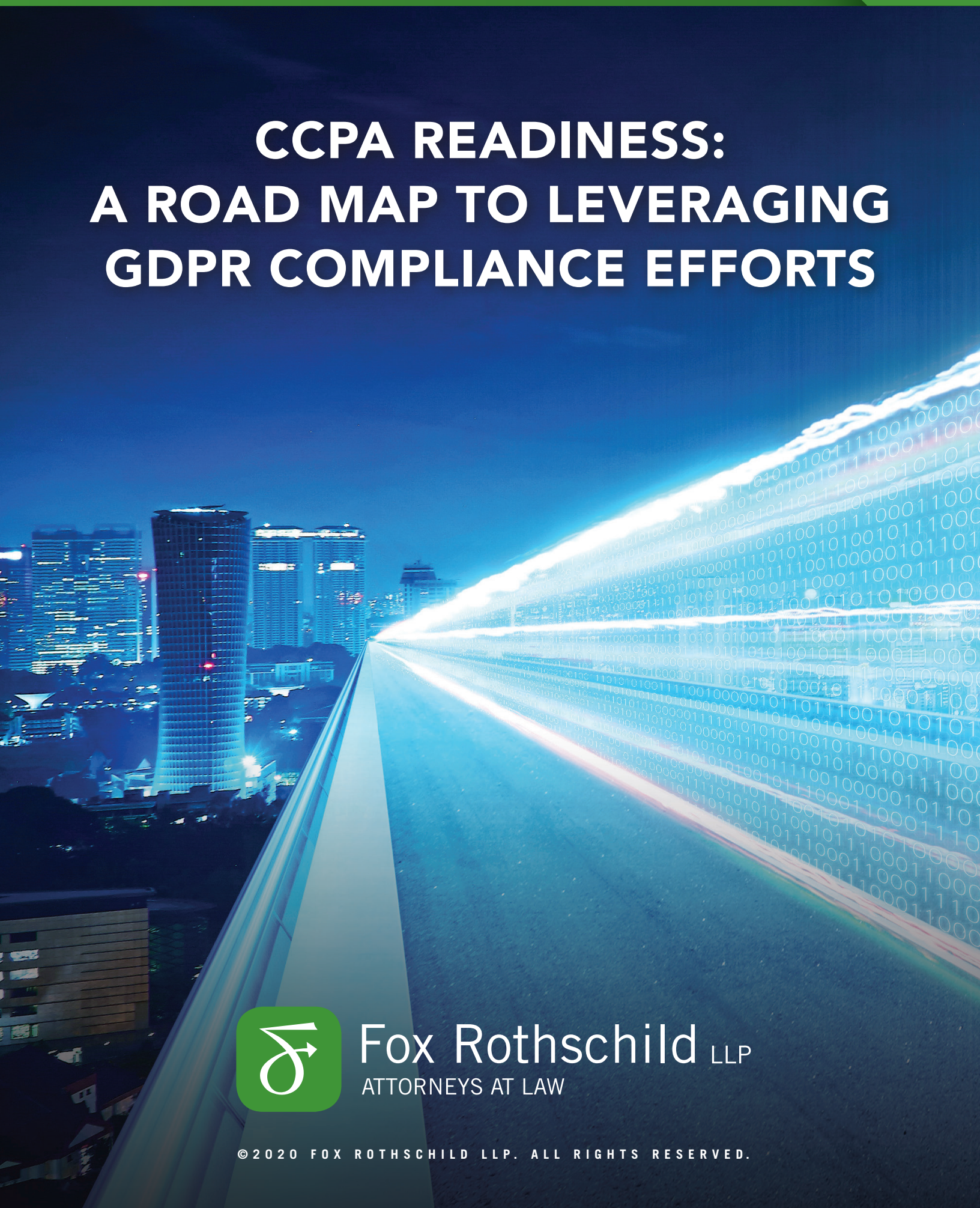
CCPA READINESS: A ROAD MAP TO LEVERAGING GDPR COMPLIANCE EFFORTS



Fox Rothschild LLP
ATTORNEYS AT LAW

The California Consumer Privacy Act (CCPA), which takes effect in 2020, has been dubbed "GDPR-Lite" or "California GDPR" because it shares many concepts and compliance obligations with the EU General Data Protection Regulation (GDPR). Both include expanded disclosure obligations and guarantee individuals the right to receive access to their information, request that their information be deleted and opt out of the sale of their information.

So, if the laws are so similar, does that mean companies that went through a robust GDPR compliance exercise before the EU privacy regulations took effect in May 2018 are also fully prepared for the CCPA?

Unfortunately, the answer is no.

If your company has already done some work toward GDPR compliance, here are the key steps you will need to take to get ready for the CCPA:

Key Contacts

ODIA KAGAN
Partner and Chair of GDPR Compliance and International Privacy
okagan@foxrothschild.com

ELIZABETH G. LITTEN
Partner and HIPAA Privacy & Security Officer
Co-Chair, Privacy & Data Security Practice
elitten@foxrothschild.com

MARK G. MCCREARY
Partner
Co-Chair, Privacy & Data Security Practice
mmccreary@foxrothschild.com

Determine Whether CCxPA Applies to You

- Are you a commercial entity (operating for profit)?
- Are you a **California-based or registered** entity OR an entity that "**does business in California?**"
  - o CCPA does not define the phrase "doing business in California," but under existing California tax laws it includes **out-of-state companies** with **no physical presence in California** that "actively engage in any transaction for the purpose of financial or pecuniary gain or profit" and meet certain financial thresholds.
- Do you **process personal information** or is personal information processed on your behalf?
- Do you **determine the purpose and means of processing** personal information?
- Do you meet any of the following **thresholds**?
  - o Generate at least $25 million in annual gross revenue [This is likely to mean generally, and not just from California]
  - o Buy, sell, share and/or receive the personal information of at least 50,000 California consumers, households or devices, per year
  - o Derive at least 50 percent of annual revenue from selling California consumers' personal information.
- Do you **control** or are you controlled by an entity meeting the above criteria and share **common branding** with it?

Continue Your Data Mapping to Include a Broader Definition of Personal Information

- **Include U.S. data**: If your U.S. and EU data was relatively segregated when you were gearing up for GDPR, you may have opted to set the U.S. data aside and concentrate only on the EU data. To prepare for CCPA, you need to **map any Personal Information that relates to California residents**. In many cases it would be a good idea to map all of your U.S. data in view of the growing number of U.S. state privacy laws that are likely to impose similar obligations regarding Personal Information in other states.
  - o As of now, **California employee information** seems to be included in the definition of Personal Information, but that may change in the near future as an amendment carving out employee data recently received a positive vote from the California Assembly's Privacy and Consumer Protection Committee.
  - o Don't forget to **include internet activity for all U.S.-facing websites**: this includes click stream, interactions with the website, browsing history, IP address and mobile device ID.
- Even if you mapped all of your data originally – update to include **additional aspects of Personal Information**, such as:
  - o **Inferences drawn** from any Personal Information to create a profile about a consumer reflecting their preferences, characteristics, behavior or attitude
  - o **"Household" and "device" data**

Consider Whether To Develop a Compliance Plan for, or Take Advantage of the Carve-Outs for Certain Types of Data Provided by CCPA

- **Publicly available** information
- Certain **medical and health** information:
  - o If you collect or sell medical or health information, assess whether it is (1) "Protected Health Information" covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or (2) the Confidentiality of Medical Information Act. Even if it is, consider whether information de-identified pursuant to HIPAA may still be "Personal Information" under CCPA.
  - o Even if it is not, consider the fact that under CCPA, health information is not entitled to a higher compliance standard in the vein of "special category data" under GDPR.
- Certain **financial information**: If you collect or sell financial information, assess whether you (1) buy or sell information from consumer reporting agencies, (2) collect or sell non-public personal information under the Gramm Leach Bliley Act (GLBA) or (3) collect or sell information covered by the California Financial Information Privacy Act.
- Personal Information under the **Driver's Privacy Protection Act**.
- Personal Information collected as part of **certain clinical trials**.

Assess and Amend Your Service Provider Agreements

- **Map all the service providers** that process Personal Information for you.
- **Amend the agreements** to include obligations such as:
  - o Use/disclose/retain only for the specific purpose of performing the services specified in the agreement.
  - o Respond in a timely manner to access and deletion requests.
  - o Provide access to information in portable and readily usable format.
  - o Operationalize "opt outs".

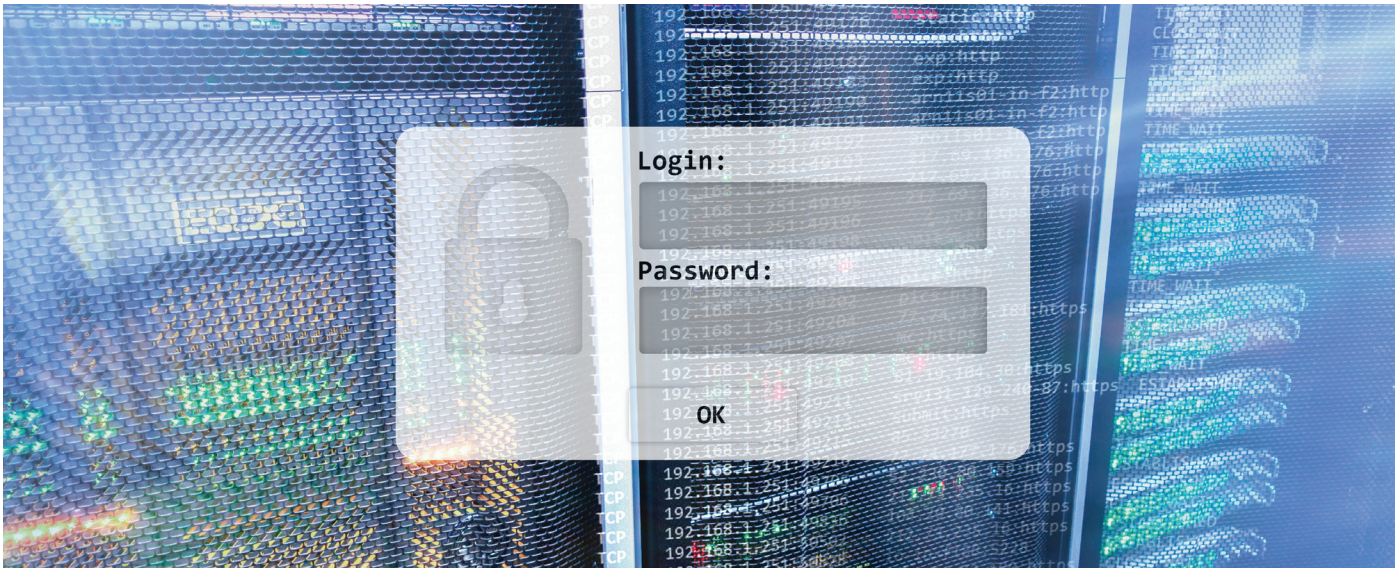
Assess and Amend Your Data Sharing Agreements

- Include requirements for a third party to **notify individuals when it intends to sell** personal information about those individuals that has been sold to it by the business, and provide the opportunity to opt out.
- If sharing **de-identified or aggregated** information, include requirements for:
  - o technical and procedural safeguards to prevent re-identification
  - o business processes to prohibit re-identification
  - o prohibition of any attempt to re-identify

Devise a Process To Verify the Identity of an Individual Making an Access, Deletion or Opt Out Request

Devise a Process to Address Access Requests

- If you **have not yet instituted a process for responding to access requests**, devise a process that includes **providing the required disclosures**:
  - o The categories of personal information you collected about the consumer
  - o The categories of sources from which the personal information is collected
  - o The business or commercial purpose for collecting or selling personal information
  - o *If you sell information*, the categories of personal information that the business sold
  - o The categories of third parties with whom you share personal information
  - o *If you sell information*, the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold
  - o *If you disclose information for a business purpose*, the categories of personal information that the business disclosed about the consumer for a business purpose
  - o The specific pieces of personal information collected about that consumer
- If you have **instituted a process for addressing access requests under GDPR**:
  - o Consider whether to **adapt the scope of access** to include only information (1) collected or sold (as opposed to "processed") and (2) only in the preceding 12 months, and whether to limit responses to just twice a year.
  - o **Adapt the disclosure** you provide with the responses to include:
- *If you sell information*, the categories of personal information that the business sold
- The categories of third parties with whom you share personal information
- *If you sell information*, the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold
- *If you disclose information for a business purpose*, the categories of personal information that the business disclosed about the consumer for a business purpose
  - o Find a **portable and readily usable format** for sending the information.
  - o Use the **CCPA timetable** of 45 days or have a 30-day GDPR timetable across the organization.
- In either case, provide **two methods individuals can use to exercise their rights**, one of which needs to be a toll-free telephone number.



Devise a Process To Address Data Deletion Requests

- If you **have not instituted a process for responding to data deletion requests**, devise a process that includes:
  - o **Knowing where** all the relevant information collected from the individual is located
  - o Assessing whether an **exception** applies to responding
  - o **Informing and educating** all the relevant stakeholders of the need for timely responses
- If you **have instituted a process for responding to deletion requests under GDPR**:
  - o Amend the deletion procedures to **apply across the board** and not only for specific legal circumstances (like GDPR).
  - o Consider whether to apply the deletion procedures to all information (like for GDPR) or **only information collected from the individual** (as CCPA requires).
  - o Consider whether to use the **CCPA timetable** of 45 days or have a 30-day GDPR timetable across the organization.
  - o Use existing GDPR exceptions to the right of erasure or utilize the **additional exceptions available under CCPA** including when data is needed:
    - To detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity; or prosecute those responsible for that activity.
    - To debug, identify and repair errors that impair existing intended functionality.
    - For uses that are "reasonably anticipated" in the context of the relationship or the purpose for providing the information.
    - **Document the process** for determining that your use falls under this exception in case it is challenged later.

Devise a Procedure for Addressing the Right to Opt Out of a Sale

- Assess which of your data sharing activities are **included in the broad CCPA definition of "sale."** This can include:
  - o Sharing for marketing/advertising purposes
  - o Sharing for a third party's analytics purposes
  - o Sharing (e.g. with data brokers) in consideration for a service or acknowledgement
  - o Any situation in which you receive a benefit you are not entitled to receive by law in exchange for the information
- Assess whether you are able to take advantage of any of the **exceptions to the definition of sale**, such as:
  - o You were directed to share the information by an individual OR an individual uses your business to intentionally interact with a third party and the agreement with the third party with whom the information is shared prohibits sharing that is not consistent with the original purpose.
  - o You share the information in order to notify a third party that an individual has opted out of the sale of his/her information.
  - o You are sharing information as necessary to perform a business purpose provided that: (1) this sharing was included in your notice and (2) the agreement with the service provider prohibits further use of the information other than as necessary for the business purpose.
  - o You are sharing the information as part of a business reorganization.
- Devise an **opt-out process** for any sharing activities you determine constitute a "sale."
- If you have a **cookie consent management platform**, consider whether to adopt that for use with California consumers or use an opt-out based tool.

Amend Your Data Portability Procedures

- If you have a GDPR process, amend the procedure to include **all situations where data access is requested** (not only data collected based on the legal bases of "contract" and "consent").

Revise Your Online Privacy Notice

- If you **have not amended your privacy notice in connection with GDPR**, amend it to incorporate the additional disclosures required by CCPA. These include:
  - o Categories of information collected – not just on the website
  - o Categories of sources from which the information has been collected
  - o Separate lists of categories of information collected, sold or disclosed over the past 12 months
  - o Purposes for which the information collected will be used
  - o If the business sells personal information, the rights to which the individuals are entitled and how to exercise them
  - o Description of your financial incentive programs
- If you **have amended your privacy notice in connection with GDPR**, further amend it to address the following issues:
  - o Include **separate lists** of categories of information collected, sold or disclosed over the past 12 months (or the fact that you have not done so).
  - o The **additional rights** to which California residents are entitled
  - o Your **financial incentive** program
- Institute a process for **amending your privacy notice every 12 months**.
- Provide a "clear and conspicuous link" titled "**Do Not Sell My Personal Information**" on the business's homepage OR create a homepage that is dedicated to California consumers.

Assess Your Financial Incentives/Loyalty Plans

- Disclose the plan/incentive in the privacy notice.
- Devise a process for getting **opt-in consent** for participation in the program.
- Ensure that your financial incentive practices are not unjust, unreasonable, coercive or usurious in nature.
- Ensure that any (1) difference in price or rate that you charge consumers, (2) different quality of goods or services or (3) financial incentives, including payments to consumers as compensation for the collection of personal information, the sale of personal information or the deletion of personal information, **are reasonably related to the value provided** to the consumer by the consumer's information.
  - o Document your analysis of the relationship between the incentive and the value provided by the information to make the rates defensible.
  - o Note: The criterion here is not explained in the law and would benefit from guidance from the California Attorney General.

Fox Rothschild LLP
ATTORNEYS AT LAW

Contacts

Odia Kagan
215.444.7313
okagan@foxrothschild.com

Elizabeth G. Litten
609.895.3320
elitten@foxrothschild.com

Mark G. McCreary
215.299.2010
mmccreary@foxrothschild.com

www.foxrothschild.com