Client Alert | Data, Privacy & Cybersecurity

UK Business Exposure To The California Consumer Privacy Act 2018 ("CCPA")

January 2020

Authors: John Timmons, Steven R. Chabinsky, F. Paul Pittman

The CCPA took effect on 1 January 2020, introducing significant compliance burdens for most businesses that collect personal information about California residents. The reach of the CCPA extends beyond California and the US; it may apply to businesses based in the UK depending on the level of interaction with California residents and their personal information. Businesses based in the UK should understand the CCPA exposure risk, since the compliance requirements differ in some material ways from the General Data Protection Regulations ("**GDPR**") and the UK Data Protection Act 2018 ("**DPA 2018**").

Which businesses are subject to the CCPA?

The CCPA applies to for-profit legal entities (or sole proprietorships) that:

- *Do business* in the State of California;
- *Collect personal information* of California consumers;
- *Determine the purpose and means of processing* California consumers' personal information; **and**
- either:
    - have annual gross revenues in excess of $25 million;
    - buy, sell, receive, or share for commercial purposes the personal information of at least 50,000 California consumers, devices or households, on an annual basis; **or**
    - derive at least 50% of annual revenues from selling the personal information of California consumers.

As the CCPA applies to for-profit entities that "*do business*" in the State of California, the CCPA has extraterritorial reach. It can apply to businesses located outside of California, and outside of the US, that satisfy the criteria set out above.

A fundamental issue for businesses based in the UK is to understand whether they "*do business*" in the State of California. The CCPA does not offer any clarity as to the meaning of this wording; however, there is case law in the US that suggests that California laws can apply to businesses established outside of the state, if California residents suffer harm in the state. In the context of California tax law, businesses without a physical presence in California have been found to be doing business in California due to online business activities.

It is likely that the CCPA would apply to a business based in the UK that collects the personal information of California residents in the context of selling goods or services to such individuals as long as the individual is physically located in California at the time the personal information is collected.

The CCPA excludes consumer personal information collected "*wholly outside of California*" from the limitations that would otherwise be applicable to its collection and sale. This might occur, for example, where a UK-based business collects the personal information of a California resident while they are visiting a physical location in the UK or accessing the business' website while in the UK.

Key differences between the CCPA and the GDPR

Businesses that are based in the UK and which are subject to the CCPA should be aware of the CCPA compliance requirements that differ from the GDPR and the DPA 2018. Some of the key differences include:

In-scope information:

The GDPR applies to the processing of "*personal data*", whereas the CCPA applies to the processing of "*personal information*". Both the CCPA and the GDPR have a clear focus on information concerning individuals; however, there are some subtle differences between the two approaches. For example, the CCPA includes within the scope of "*personal information*" information that can be linked to a particular household; whereas the GDPR is only concerned with information relating to an individual. In addition, the CCPA definition applies to information that is "*capable*" of being associated with, or that could reasonably be linked to, a person. This is broader than the GDPR, which requires that personal data be information that can identify an individual, and not merely information that is capable of being associated with, or linked to, an individual.

Relevant individuals

The CCPA focuses on "*consumers*", being individuals who are California residents. The GDPR focuses on "*data subjects*", being any individual who is the subject of personal data. The GDPR is not concerned with the residency or citizenship status of the relevant individuals, and is therefore much broader in its scope than the CCPA with respect to the individuals who benefit from the protection it offers. For example, a business based in the UK that processes the personal data of individuals resident in New York must comply with the GDPR and the DPA 2018 with respect to the processing of the personal data relating to such individuals.

Disclosure and transparency requirements

Like the GDPR, the CCPA requires that businesses disclose certain information to individuals regarding the manner in which their personal information is used. Most of the information that the CCPA requires businesses to disclose is also required by the GDPR. There are, however, some differences between the disclosure and transparency requirements of the CCPA and the GDPR. For example: (i) if personal information is to be sold by a business, the CCPA includes very prescriptive obligations with respect to the information that must be provided to consumers; and (ii) some of the disclosures required by the CCPA are limited to activities of the business in the previous 12 months; whereas the GDPR imposes no such limitation.

Individual rights

Both the GDPR and the CCPA confer rights on the individuals whose information is being processed. The rights conferred by the GDPR are greater in number and more extensive in scope. For example, although the GDPR and CCPA allow individuals to request that businesses delete their personal information, the exceptions that businesses can rely on as set out in the CCPA so as not to give effect to a deletion request are broad enough to potentially eliminate a consumer's right in this respect.

Prohibit Sale of Personal Information

Unlike the GDPR, the CCPA provides consumers with a specific right to prohibit a business from selling their personal information, which can be exercised at any time. The GDPR does not expressly provide for such a right. Although EU data subjects may limit or challenge the processing of their personal data, such challenges are limited and may be usurped where a business establishes a need to process the personal information. For example, a business that makes personal information available to a third party without restricting the third party's ability to further process the personal information, in exchange for services or a reduction in fees, may

be subject to a consumer opt-out request prohibiting such an exchange under the CCPA. However, an EU data subject may not have a similar right, except in limited circumstances.

For a more detailed overview of the differences between the CCPA and the GDPR, please see our guide, which can be found here.

Leveraging GDPR and DPA 2018 compliance efforts

Since the text of the GDPR was finalised in 2016, and following the introduction of the DPA 2018 in May 2018, businesses have invested significant resources in complying with the extensive compliance requirements. Further effort has been required to react to the guidance issued by the European Data Protection Board and the fines imposed by data protection regulators for non-compliance.

Many businesses are already leveraging these efforts and are applying GDPR compliance structures globally. Adopting a "*highest common denominator*" approach generally helps to streamline efforts to comply with national data protection laws in countries located outside of the European Union. This is an effective strategy since the requirements of the GDPR typically far exceed the requirements of data protection laws in non-European Union countries.

Businesses in the UK that are subject to the CCPA should consider adopting a similar approach and seek to leverage existing GDPR and DPA 2018 compliance measures. Such measures will invariably support compliance with the CCPA. Of course, some changes will be necessary and specific requirements of the CCPA will need to be addressed. Importantly, a business should anticipate needing to be flexible in its implementation of, and adjustments to, data privacy practices required under the CCPA. The final CCPA regulations have yet to be finalised and could differ significantly from the existing law.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000