PAUL HASTINGS

PH PERSPECTIVES

November 2019

Follow @Paul_Hastings

CCPA: My Business Isn't Based In California – Should I Be Taking Action?

By Sarah Pearce, Behnam Dayanim, Ashley Webber & Claire Blakey

Data privacy is fast becoming one of the most widely regulated areas, with the last two years the most influential of all. The introduction of the General Data Protection Regulation (the "GDPR") changed the privacy landscape globally. In part, this was due to its extra-territorial application, meaning certain businesses outside the EU fall within its scope and must comply with its provisions. Organisations worldwide were suddenly faced with having to take varying degrees of action to comply with the GDPR, and now certain of these organisations, plus many more, are looking towards compliance with the next significant privacy legislation—the **California Consumer Privacy Act** (the "CCPA"), Cal Civ. Code § 1798.100 *et seq.*

On 1st January 2020, the CCPA will take effect (although the Attorney General will not begin enforcing the law until six months after the final implementing regulations are published, or July 1, 2020, whichever comes first). The California Attorney General recently released draft implementing regulations for the CCPA, which are open to initial public comment until December 6, and should be finalised in the spring of 2020.

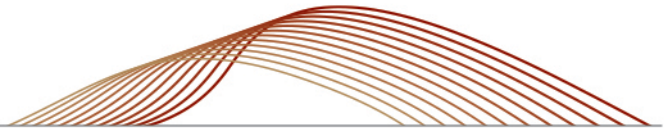
The CCPA gives California residents important new rights in relation to their personal data. Like the GDPR, the CCPA also appears to have extra-territorial effect (see below for further discussion), and organisations should therefore conduct an analysis to confirm whether they will fall within remit of the CCPA and if so, what steps, if any, they need to take towards compliance.

The Basics

The CCPA provides protections and rights in relation to the "personal information" of California residents. A California resident is defined as: (i) an individual who is in the State for other than a temporary or transitory purpose; or (ii) an individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. In the simplest terms, a resident is an individual who lives in California and the rights provided under the CCPA do not cease to exist when the individual leaves California for a provisional period, such as a holiday. However, the CCPA caveats this slightly by clarifying that it does not apply to the collection or sale of personal information "*if every aspect of that commercial conduct takes place wholly outside of California*".[1]

The definition of "resident" is different to that of the "data subject" under the GDPR. Unlike the CCPA, the GDPR does not, by default, link applicability of its provisions to the geographical location of the data subject—if an organisation is based in the EU and processes personal data of data subjects based outside the EU, such organisation would have to comply with the GDPR.

The CCPA requires that an organisation "*do [ ] business in the State of California*" for it to apply. The phrase "*doing business in the State of California*" is not defined in the CCPA, though the best interpretation of the CCPA's reach is that it can apply to businesses **without a physical presence**



in California so long as they collect the personal information of California residents, as defined above. The CCPA could therefore apply, for example (subject to satisfying the additional criteria identified below), to an online retailer based in the UK that markets and sells its goods globally, including to California residents.

The definition of "personal information" under the CCPA, whilst worded differently, is consistent with the definition of "personal data" under the GDPR. "Personal information" is defined in the CCPA as "*information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*".

Who must comply?

In order to fall within the scope of the CCPA, an organisation must:

1. **collect** the personal information of California residents (either directly or through a third party);
2. be "**for-profit**", therefore excluding, for example, not-for-profit charities or public authorities;
3. "**do** [ ] **business in the State of California**";
4. determine the **purposes and means of processing**, like a controller under the GDPR; and
5. meet one of the following **conditions**:
    a. the business must generate annual gross revenue in excess of $25 million;
    b. the business must receive or share personal information of more than 50,000 California residents annually; or
    c. the business must derive at least 50 percent of its annual revenue by selling the personal information of California residents;

    or any entity that controls or is controlled by a business that meets the requirements above, and that shares common branding with such a business.

For organisations that must comply, what does the CCPA require they do?

What does compliance with the CCPA entail? And are there any key differences with the GDPR? In the main, the CCPA is focused on increasing the rights of California residents in relation to their personal information. We have highlighted the key provisions of the CCPA below and identified material differences with the corresponding obligations under the GDPR.

CCPA Provision	GDPR Comparison
Right to know about personal information collected, disclosed, or sold **1. Notice at Collection** The CCPA requires businesses to present to consumers a "*notice at collection*", either at or before the time they collect a consumer's personal information. This notice must contain: (i) a list of the categories of personal information about consumers to be collected, and the business or commercial purpose(s) for which it will be used; (ii) if the business sells personal information, the link titled "Do Not Sell My Personal Information / Info" (or for offline notices, the web address for the webpage to which it links); and (iii) a link to the business's privacy policy (or for offline notices, the web address of the business's privacy policy). If a business intends to collect additional categories of personal information, the business must provide a new "notice at collection". If a business intends to use personal information for a purpose not previously disclosed in the notice, the business must directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for the new purpose. **2. Privacy Policy** A business must notify consumers of the following: (i) a list of the categories of personal information the business has collected about consumers in the preceding 12 months (as well as the categories of sources and the business or commercial purpose for collection of the information); (ii) a list of the categories of third parties with whom the business has shared personal information in the preceding 12 months; and (iii) a list of the categories of personal information that the business has sold or disclosed for a business purpose in the preceding 12 months (or the fact that the business has not sold or disclosed this information). The privacy policy must also describe the rights of consumers regarding their personal	Less information has to be provided to the individual under the CCPA; a compliant GDPR Article 13 notice would include the information required by the CCPA. However, the GDPR does not require the following which should therefore be actioned when applicable: **(i) notice and policy to be updated every 12 months; and (ii) express notice given for third party sale of information**. In relation to the "*notice at collection*" requirement for the CCPA, most GDPR compliant businesses provide their privacy policy at collection of the data to satisfy the Article 13 requirements. Therefore, if the GDPR compliant privacy policy is provided at, or before, collection of the data, this will also satisfy the CCPA requirement.

information (as well as how to exercise these rights). It must be updated **at least every 12 months**.	
Right to request specific information about the personal information collected, sold, or shared about that consumer Consumers have the right to request that a business collecting a consumer's personal information disclose to that consumer: (i) the categories of personal information it has collected about that consumer in the preceding 12 months (as well as the categories of sources and the business or commercial purpose for collecting the personal information); (ii) the categories of third parties with whom the business shared the personal information; and (iii) a list of the categories of personal information that the business has sold or disclosed for a business purpose in the preceding 12 months (or the fact that the business has not sold or disclosed this information). Businesses must acknowledge the receipt of consumer requests within **10 days**, and then respond within **45 days** (though this timeline can be extended once when "reasonably necessary" by an additional 45 days, if the business notifies the consumer before the first 45 days are up). The information must be provided free of charge. There are several exemptions permitted to complying with such a request, certain of which are similar to those under the GDPR. **Right to request the specific pieces of personal information collected about the consumer in the preceding 12 months** The CCPA requires a business provide the data electronically in a readily useable format that allows the consumer to easily transmit the information to another entity, which is why some have compared this right to the GDPR's right of data portability. The same timeframe applies to respond.	The right of access under the CCPA is fairly similar to that under the GDPR, although the range of information to be provided in response to an access request under the GDPR is arguably broader and, in most circumstances, it must be provided within a shorter period of time, i.e. **30 days**. If the business is established in the EU and is processing the personal data of individuals in California, it will currently be required to comply with the GDPR in relation to such individuals, even though they are outside the EEA. Post-implementation of the CCPA, if the same entity of a business were to receive an access request from a California resident, it is not clear whether this should fall within the remit of the CCPA or the GDPR, and to avoid the risk of breaching the stricter GDPR provisions in this regard, **the business should treat the request as a GDPR request**. If the business is based outside the EEA but has to comply with the GDPR in respect of its EU personal data, it would not have to comply with the GDPR in respect of an access request from a California resident, but instead should comply with the CCPA. **Right of data portability** The CCPA right is not as wide as that under the GDPR. The GDPR right of portability is a distinct right which allows, in certain circumstances, for a data subject to receive, and transmit/have transmitted to another controller, their personal data in a commonly used, machine-readable format.

Right to request deletion of personal information A consumer has the right to request deletion of personal information that a business has **collected** from them. This extends to service providers (the equivalent of a GDPR processor) and any other third parties to which the business has provided/sold the personal information. A business must respond, free of charge, in the same timeframe as above. There are several exemptions permitted to complying with such a request, certain of which are the same as under the GDPR.	The right of deletion under the CCPA is similar to the right of erasure under the GDPR, although the GDPR requires all data be deleted (if right is exercisable), as opposed to only that "collected" from the consumer, and in most circumstances, within a shorter period of time, i.e. **30 days**. If the business is established in the EU and is processing the personal data of individuals in California, it will currently be required to comply with the GDPR in relation to such individuals, even though they are outside the EU. Post-implementation of the CCPA, if the business were to receive an eraser request from a California resident, it is not clear whether this should fall within the remit of the CCPA or GDPR, and therefore to avoid the risk of breaching the GDPR having stricter provisions in this regard, **the business should treat the request as a GDPR request**. If the business is based outside the EU but has to comply with the GDPR in respect of its EU personal data, it would not have to comply with the GDPR in respect of an eraser request from a California resident, but should comply with the CCPA.
Right to opt-out of the sale of personal information The CCPA defines "sale" as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration". Consumers aged **16 and older** have the right to opt-out of their personal information being sold and to opt-out from the subsequent sale of the personal information by a third party that received it after an initial sale. If a business sells personal information, in addition to information in the notice as stated above, it must also **post a "*Do Not Sell My Personal Information*" link** (using this phrase) on its homepage, which allows consumers to easily	The CCPA right to opt-out of the sale of personal information is similar to the right to object under the GDPR, however the right under the CCPA is narrower in scope in that it relates only to the ***sale*** of personal information. The right to object under the GDPR allows a data subject to object to any processing if based on legitimate interests or if the processing is direct marketing. The GDPR does not expressly state that a link of the nature explained must be provided; therefore, if an organisation does sell information that is currently subject to the GDPR and will also be subject to the CCPA, it must **include such a link**.

exercise that right of opting-out. Businesses must honour "Do Not Sell" requests within 15 days and inform any third parties who received the personal information of the request within 90 days. Note that businesses cannot sell the personal information of consumers **under the age of 16** unless they or their parent or guardian (in the case of consumers under 13) have affirmatively authorised the sale of their personal information.	
Right to non-discrimination for the exercise of a consumer's privacy rights The CCPA states that a consumer cannot be discriminated against because they choose to exercise their rights under the CCPA. For example, the business cannot charge a fee because they exercised a right of access.	Whilst there is no equivalent express right under the GDPR, it is implicit from the principles of the GDPR that individuals must be protected from discriminatory consequences derived from processing their data. For example, Article 5 states data must be processed "fairly", and when a business opts to rely on consent as its lawful ground, it must be a "free" consent, meaning it cannot be conditional. Given the right under the CCPA is one which should be complied with as a principle under the GDPR, no further action need be taken by a GDPR-compliant business.
Vendor Contracts The CCPA regulates the role of a "Service Provider" acting on behalf of a business. A "Service Provider" is defined as a *"for profit [organisation]* ***that processes information on behalf of a business*** *and to which the business discloses a consumer's personal information for a business purpose* ***pursuant to a written contract****, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business*". Therefore, the CCPA requires a written contract to be in place between a business and its service provider that governs the processing of	The requirement to have a contract in place is similar to the provision under the GDPR which requires organisations in a controller/processor relationship to enter into a written contract. However, the GDPR requires significantly more provisions be included, as a minimum, in said written contract. Given the high standard of the GDPR in this regard, a written contract in place between a controller and processer under the GDPR would likely satisfy the requirements of the CCPA. However, we would recommend reviewing the agreement to ensure the processing is adequately covered for CCPA purposes. Further, notwithstanding whether a relationship with a vendor satisfies the controller/processor relationship of the GDPR, **all vendor relationships under which data is processed should be reviewed to confirm whether a written contract is required in order to comply with CCPA**.

the personal data by the service provider on behalf of the business.	
Civil Enforcement Civil penalties can be imposed but only as a result of an action brought in the name of the people of the State of California by the Attorney General. There is no right of private claim absent a data breach (see below). The penalty imposed will depend on the violation and could be up to: (i) $2500 per violation; or (ii) $7500 per incidental violation. There is no maximum imposed on the number of violations that can be grouped together, so there is no cap on the overall monetary penalty.	The enforcement position is rather different under the GDPR. Firstly, penalties can be imposed by a regulatory (data protection) authority. Secondly, the possible fines are as follows and depend on which GDPR provision is violated: (i) 2% of annual global turnover or €10million, whichever is higher; or (ii) 4% of annual global turnover or €20million, whichever is higher. The sum of the penalty itself is also discretionary to a degree, as it will depend on the nature of the breach. What is most important to flag here is that, in certain circumstances, if a business is in breach of either one of the legislative acts, it may well also be in breach of the other. This will mean potentially being exposed to financial penalties under both regimes.
Private Right of Action for Data Breaches If a consumer's "*nonencrypted and nonredacted personal information*" is subject to an "*unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information,*" the consumer is entitled to initiate a civil action. The amount of damages can be an amount not less than $100 and not greater than $750 per consumer per incidental or accidental damages, whichever is greater. Class (or group) claims are not prohibited. Such an action can only be brought if, prior to initiating the action, the consumer provides the business with 30 days' written notice identifying the specific provisions of the CCPA that the consumer alleges have or are being violated. If the violation is cured by the business within the 30 days, and the business provides a statement that no further violations will occur, no action can be brought.	Similar to the right for data subjects under the GDPR but the right under the GDPR is broader in that data subjects can take action for **any** violation of the GDPR. Further, the GDPR does not cap the damages payable. The possibility of class (or group) claims being brought by data subjects will depend on the national law. There is no specific action a GDPR-compliant business need take in this regard, but if it has a policy or procedure relating to individual claims, it may wish to update the document to include details regarding the right to claim under the CCPA. **Note that depending on the violation, an individual could bring a claim under both the CCPA and GDPR.**

We have not reviewed all provisions of the CCPA but have instead focused on those we consider to be the most significant, those which best demonstrate the purpose of the legislation (i.e. to increase the rights of individuals in relation to their personal information), and the interesting nuances as regards the GDPR.

Whilst the purpose of the CCPA is consistent with the key driver behind the GDPR, the CCPA comprises fewer obligations than the GDPR. The CCPA is also narrower in scope, with the GDPR seeking to regulate ***all businesses*** that process personal data as opposed to only those satisfying certain criteria. Furthermore, a number of GDPR provisions focus on business practices as a whole (e.g. record-keeping requirements), rather than individuals' rights alone.

If my business is compliant with the GDPR, what actions should it be taking?

As the above table demonstrates, there are striking similarities between the CCPA and the GDPR. In our view, organisations already in compliance with the GDPR will likely be in a strong position when faced with complying with the CCPA.

As part of any GDPR compliance project, businesses globally will have carried out data mapping exercises in an attempt to fully understand their use and storage of data, how it is processed, why it is processed in such a way, and who it is shared with. By carrying out such an exercise, businesses were able to identify areas of risk in relation to personal data within their business and initiate a plan to mitigate said risks and ensure compliance. The plan will likely have included steps such as updating privacy notices, reviewing and, where relevant, updating agreements with third parties, appointing data protection specialists, reviewing marketing lists, and cleansing potentially unlawful data.

Organisations that completed compliance projects for GDPR will be standing in good stead when assessing CCPA compliance. We recommend such organisations use the CCPA as an opportunity to review and reassess their compliance with the GDPR and data privacy practices within their business generally to ensure they are operating at the highest global privacy standard. In doing so, possible areas of improvements may be identified, both from a GDPR and a CCPA perspective.

The underlying message of the CCPA is the same as with the GDPR—data privacy and security is, and will continue to be, a fundamental concern globally, both from a legal and commercial perspective, and organisations should make certain sooner rather than later that data privacy and security is a key pillar in the foundations of their business.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

London

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Ashley Webber
44.020.3023.5197
ashleywebber@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Claire M. Blakey
1.202.551.1859
claireblakey@paulhastings.com

[1] "*if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold.*" Cal. Civ. Code § 1798.145(a)(6).

Paul Hastings LLP

PH Perspectives is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2019 Paul Hastings LLP.