Guidance note

The global evolution of data protection law - are you meeting your obligations?

The introduction of the California Consumer Privacy Act (CCPA) at the beginning of the year continues a global trend of law-makers introducing new and more stringent rules for companies using individuals' data.

Whilst CCPA brings data protection into sharper focus for many US businesses, it shouldn't be disregarded out of hand by businesses outside the US, many of whom are still in the process of adapting to GDPR. Indeed, California is annually ranked between fifth and seventh in terms of global market share. Thus, changes in California law often have an international impact. In fact, CCPA's introduction is a strong indication for companies that simply aligning with the rules of GDPR may no longer be enough to ensure data protection compliance.

Last year's €50 million fine of Google by the French data protection authority is just one example of GDPR enforcement action currently being taken by regulators across Europe and enforcement action by the Californian Attorney General for violations of CCPA will likely commence from July this year. Clearly, with these legislative and enforcement developments, the risk profile of not meeting data protection obligations is changing, especially for those businesses operating internationally.

The global reach of data protection law

Continuing from CCPA, and in addition to further US state laws, additional changes to data protection laws are anticipated around the world. These include the Personal Data Protection Bill in India, changes to Singapore's Personal Data Protection Act and the separation of UK data protection law from the GDPR following the UK leaving the EU.

With data protection laws increasingly characterised by their extra-territorial effect, data protection functions are, or should be, responding to this evolving global rulebook on data protection. One of the big challenges to doing this is that the rulebook is not globally uniform, with jurisdictions creating their own various interpretations of common data-related themes that include increasing transparency, strengthening rights of individual data subject and putting in place controls for transfers to third parties.

Whilst each legislatures' application of these themes are different, the consequences of getting them wrong are generally similar – risking hefty enforcement penalties, litigation and costly reputational damage.

This is unlikely to be welcome news, especially for those General Counsels and Data Protection Officers that are tasked with leading GDPR data protection compliance alongside other job responsibilities.

CCPA – do you need to comply?

With CCPA having taken effect on 1 January of this year, for many organisations the data protection hot topic is determining what, if anything, needs to be done to comply with CCPA.

Those outside of California are likely to ask – *does CCPA apply to my business?*

In short, you cannot assume CCPA does not apply to you because you do not have a physical presence in California. Similar to GDPR, CCPA can apply to processing of personal data regardless of the nationality or geographic location of organisations involved or where the processing actually takes place.

CCPA generally applies to for-profit businesses doing business in California that collect or share Californian residents' personal information and meet any one of the following three thresholds: -

- annual gross revenues in excess of twenty-five million U.S. dollars;
- alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more California residents, households, or devices; or
- derive 50% or more of annual revenues from selling California residents' personal information.

Note, even if your business on its own does not meet one of the criteria, CCPA still applies to businesses that jointly with others, meet one of the thresholds. And it also applies to any business that controls or is controlled by, and shares common branding with, a business that meets the criteria.

CCPA – how to respond?

For organisations that already have to comply with GDPR, helpfully, there are a number of similarities between the requirements under GDPR and CCPA, including:

- existing GDPR-compliant privacy notices are likely to already include much of the information that must be provided to individuals under CCPA; and
- GDPR subject access request procedures and tools are likely to be useful when approaching CCPA's individual rights, such as rights of access and erasure.

However, it is not as simple as compliance with GDPR being equivalent to CCPA.

There are some substantial differences between the two laws that need to be addressed when designing a compliance response to CCPA, including:

- With the exception of breach rights and right to notice, CCPA currently only applies to consumers' personal information (with employee and business to business information anticipated to be within scope from 2021). Additionally, CCPA incorporates information about households as part of its definition of "personal information," which goes beyond information about individuals.
- CCPA requires that specific information, controls, and rights relating to the "sale" of personal information are provided to individuals – these are unlikely to be addressed by data protection practices designed to comply with GDPR. The definition of "sale" in the CCPA is quite broad, and encompasses any sharing, disclosing, or communication of personal information to another business or third party for monetary or valuable consideration.
- CCPA data subject rights to know are generally subject to a limitation that they only apply to data collected in the prior 12 months – no such time restriction applies under GDPR.
- Unlike GDPR, there are no obligations to appoint data protection officers or representatives or to report data breaches within a certain time-frame under CCPA. However, the CCPA does require appropriate training for those handling data subject requests to ensure that those individuals know how to direct consumers to exercise their rights under the CCPA.

The table below takes a closer look into how some of the requirements under CCPA and GDPR compare and contrast:

	GDPR	CCPA
What constitutes personal data?	Under GDPR, personal data includes information relating to natural (living) persons who: • can be identified or who are identifiable, directly from the information in question; or • who can be indirectly identified from that information in combination with other information	CCPA defines personal information as *"information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."* This definition is generally broader than under GDPR. However, unlike GDPR, there are exclusions, such as personal information covered by other laws, some publically available information and clinical trial data. Additionally, personal information does not include deidentified or aggregate information. It also does not include publicly available information that is lawfully made available from federal, state, or local government records.

	GDPR	CCPA
Registration requirements and appointments	Under GDPR, a Data Protection Officer must be appointed where data controller's processing meets certain thresholds, including for all public authorities. Data controllers may be required to register with relevant supervisory authorities. In the UK, data controllers must pay an annual fee to the UK's supervisory authority, the Information Commissioner, unless one of a few limited exemptions apply. It is generally necessary to appoint a representative in the EU (and likely the UK under UK GDPR) if processing personal data without local presence or "establishment".	Under CCPA, there are no equivalent Data Protection Officer or company representative requirements. It is not generally required to notify or register with the Californian Attorney General – this is only mandatory for businesses that act as data brokers and authorised agents who consumers may authorise to act on their behalf to exercise data subject requests.
Privacy information that needs to be provided to individuals	A strict list of information must be provided by controllers to individuals at the time of collecting data or no later than one month after obtaining personal data from a third party. Such information includes details about the identity of the controller, data protection officer, details of data collected, purposes of data processing, legal bases being relied upon, transfer information, periods of retention, along with details of data subject rights.	CCPA requires much of the same information is provided to individuals but also requires additional information relating to "selling" of personal information. This includes providing details of the individual's right to opt out of sale by the business that has collected the information and third parties that have subsequently received it. A "Do not sell my personal information" link must be included on the business' homepage. CCPA requires that privacy policies are updated at least every 12 months, whereas no time period is specified under GDPR.
Rights granted to individuals	Under GDPR, rights available to individuals in respect to their personal data include - the right to: access data, object to processing, rectify data, restrict processing, withdraw consent to processing, the deletion of personal data and to data portability.	CCPA includes many of the same rights as GDPR, but there are subtle differences. For example, the data access right is subject to a limitation that it only applies to data collected in the prior 12 months. Consumers must also have the right to opt out of personal information being "sold" to third parties under CCPA. If information is being shared with a third party that has the right to re-sell that information, explicit notice and the ability to opt-out must be provided to the consumer. In addition, CCPA includes an express right that individuals must not be subject to discrimination for the exercise of their rights under the data privacy law, including being denied goods or services or being provided with poorer services and/or higher prices.
Obligations in respect to data breaches	GDPR requires that controllers report certain data breaches to the regulator without undue delay and within 72 hours.	The CCPA data breach statutory damages provisions supplement California breach law, which requires reporting to the Attorney General for any breach affecting more than 500 California residents, and which also requires that data breaches must be disclosed in the most expedient time possible and without unreasonable delay. Further, the CCPA provides a model security breach notification form for businesses to use, and creates a minimum recovery of $100 (or up to a maximum of $750) per individual per incident or actual damages, whichever is greater.

	GDPR	CCPA
Restrictions on transferring data	Under GDPR, it is necessary to have lawful basis to disclose personal data to any third parties, and failure to do so may make the processing unlawful for both the disclosing and the recipient parties. Transfers of personal data outside the EEA are prohibited unless appropriate safeguards have been put in place, such as an adequacy decision by the European Commission in respect to the recipient country or standard contractual clauses (in a form approved by a supervisory authority) being in place between the controller and the recipient.	There are no geographic transfer restrictions equivalent to those under GDPR. Under CCPA, there are restrictions surrounding the sharing of information with service providers, to whom sharing of personal information is not considered a "sale" (see row below). Additionally, the selling of personal information, which includes *"renting, disclosing, releasing, disseminating, making available transferring, or otherwise communicating personal information"* to third parties is only permitted where consumers have not exercised their right to opt-out of their data being sold.
Contracts with third-parties	Controllers must put in place a binding contract with third parties that process personal data on their behalf (known as processors). Controller-processor contracts must include certain terms, including a restriction on the processor to only process the personal data on the instructions on the controller, an obligation on the processor to ensure that adequate security protections are in place and a requirement that the processor deletes or returns disclosed personal data at the request of the controller.	Under CCPA, contracts with third parties involve those with service providers and those involving a sale of personal data. For the disclosure of personal information by a business to a service provider (i.e., to process the data on behalf of the business), such disclosure must be pursuant to a written contract and that contract must prohibit the recipient 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 internal use to build or improve the quality of its services, to detect data security incidents, or to protect against fraudulent or illegal activity. For agreements involving sales (similar to a controller-controller agreement), businesses must provide a link where data subjects can opt-out of such sharing. Note, it is not considered a sale where the data subject knows and directs one controller to intentionally disclose data to another.
Who enforces?	The European Data Protection Regulator for the EU and each member state appoints its own supervisory authority to enforce GDPR – this is the Information Commissioner in the UK.	The California Office of the Attorney General enforces CCPA – there is no separate dedicated data protection regulator in California at this time.

Where CCPA applies, the differences between GDPR and CCPA highlight that an existing GDPR data protection function will likely need to adapt and evolve to meet the requirements of CCPA. In particular, incumbent GDPR Data Protection Officers should be wary of an expansion of their remit to include CCPA without due consideration of how they will meet the requirements of CCPA and also continue to meet their obligations under GDPR.

Costs of non-compliance?

Not complying with CCPA risks financial consequences. These range from monetary penalties for non-compliance through to litigation costs arising from civil action by affected individuals or potentially breach of contract claims by customers or suppliers.

CCPA penalties are calculated on a different basis to GDPR administrative fines issued by European regulators. CCPA fines take the form of civil penalties issued by a state court, with actual penalties being up to $2,500 for each unintentional violation and $7,500 for each intentional violation. Although, this may sound like a trivial amount relative to possible penalties under GDPR, there is no maximum cap for multiple penalties stemming from the same violation. An enforcement action for non-compliance may be triggered by a data breach, but may also be triggered by failure to properly manage data subject requests. Given that many businesses manage the personal data of thousands of consumers, CCPA non-compliance could result in the mishandling of hundreds of thousands of data records and, thus, multi-million dollar fines. On the other hand, compliance with the CCPA may in some instances provide protection against Unfair Competition Law and Consumer Legal Remedies Act lawsuits regarding alleged improper treatment of data.

GDPR and CCPA are similar in that they envisage that affected individuals can seek damages for non-compliance. The cause of action available to 'data subjects' under CCPA is narrower than GDPR - it only relates to data loss situations, such as cyber-attacks. And it requires that the data subject provides the business 30 days' written notice. If the business cures the event within 30 days, then no action for individual or class-wide statutory damages may be initiated. In assessing the amount of statutory damages, courts will consider the circumstances of the case.

With both GDPR and CCPA now in place, class action law firms will likely be feeling optimistic that they have a healthy pipeline of work both sides of the Atlantic.

It goes without saying that data protection failings anywhere in the world will likely be damaging to an organisation's reputation. With data protection's close association with trust, being found non-compliant with either CCPA or GDPR could be heavily punished by both customers and suppliers.

What's next with global privacy?

With work already underway to amend and expand the remit of CCPA, we can expect the trend of new and more comprehensive data protection laws being introduced to continue. Other recent and upcoming developments in international data protection regulation include:

- India's draft Personal Data Protection Bill 2019 introduced in December 2019
- Data breach notification and data security legislation recently passed in New York in October 2019
- Data protection laws regarding privacy or security approved in Maine, Nevada, Massachusetts, Ohio, and Colorado in 2019
- Draft data protection legislation proposed in Washington, Illinois, Massachusetts, Minnesota, Nebraska, New Hampshire, New York, South Carolina, Virginia, and Wisconsin during January 2020
- Draft Data Transparency and Privacy Act brought to Illinois Senate in January 2020
- Amendments to Hong Kong's Personal Data (Privacy) Ordinance proposed in January 2020
- Draft bill amendments to Singapore's Personal Data Protection Act anticipated early 2020
- The Australian Consumer Data Right effective 6 February 2020
- Thailand's Personal Data Protection Act anticipated to be effective from May 2020
- Brazil's General Data Protection Law expected to take effect from August 2020
- A revised proposal of the European E-Privacy Regulation (initially proposed in January 2017) anticipated during 2020
- UK GDPR to be effective in the UK on 1 January 2021 following the end of the agreed Brexit transition period

How to structure your response to global data protection

For organisations that have not already done so, now could be a good time to think about evolving their existing GDPR data protection functions in order to meet their global compliance obligations.

Practical steps to achieving this are:

- Defining and categorising the different types of data your organization holds, with consideration of collection portals and storage.
- Mapping organisational data flows to understand likely impact of changes to international data protection laws.
- Reviewing existing resourcing of data protection compliance - assessing internal or outsourced resourcing options - and considering developing a holistic global data protection function.
- Preparing a data protection strategy to set out longer terms objectives and goals in relation to responding to international developments in data protection law – is the intention to be merely compliant or seek a competitive edge with data protection?
- Ensure appropriate and regular training on updated compliance requirements for employees.
- Recordkeeping of all compliance efforts, including required recordkeeping of data subject request materials.

If GDPR brought data protection to the attention of the board, CCPA should, at a minimum, remind the board that GDPR was just the beginning.

Who to contact:

David Varney
Head of GDPR, Burges Salmon

T +44 (0) 117 902 7261
E david.varney@burges-salmon.com

Jeremy Dickerson
Head of Technology and Communications practice, Burges Salmon

T +44 (0) 117 902 2728
E jeremy.dickerson@burges-salmon.com

Eva Pulliam
Partner, Arent Fox

T +1202.857.6323
E eva.pulliam@arentfox.com

Christine Chong
Associate, Arent Fox

T +1415.757.5517
E christine.chong@arentfox.com

GDN0054