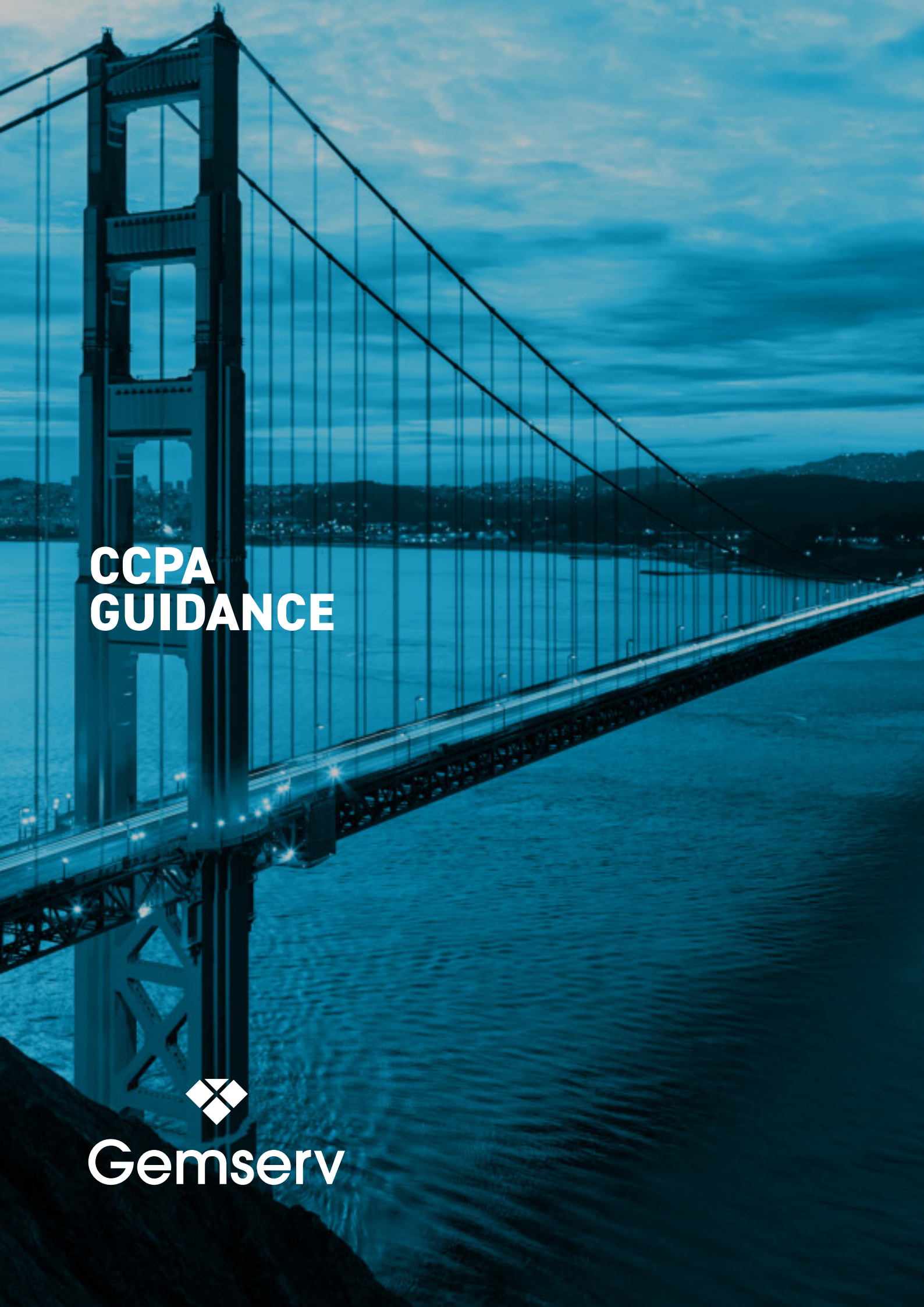


CCPA GUIDANCE

Gemserv

THE PURPOSE OF THE GUIDANCE 3

On 28 June 2018, California enacted a comprehensive consumer privacy law “the California Consumer Privacy Act of 2018” (CCPA), which will come into effect on 1 January 2020, although the Attorney General of California shall not bring an enforcement action until 6 months after the publication of the CCPA’s implementing regulations or by July 1, 2020. The CCPA introduces new privacy rights for consumers that will force certain companies conducting business in California to implement structural changes to their privacy governance. Given its extraterritorial reach like the General Data Protection Regulation (GDPR), the CCPA will considerably have a global impact on organisations that collect and process personal information of Californian residents.

As such, this guidance aims to provide clarity to organisations affected by the CCPA on its key provisions and the measures organisations should take to implement them.

THE SCOPE OF APPLICATION

A — WHEN THE CCPA APPLIES TO BUSINESS?

The CCPA does not cover every business, but covers the vast majority of Californian, US or international organisations that collect the personal data of Californians. The act will apply to your organisation if it is a legal entity that:

- Does business in California, regardless of whether it has a physical presence/office/establishment/company registration in the state. An organisation appears to "do business in California" simply if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit within the state, and;
- Collects personal information from Californian residents, or buys or sells personal information of Californian residents, and determines the purposes and means of processing consumer's personal information

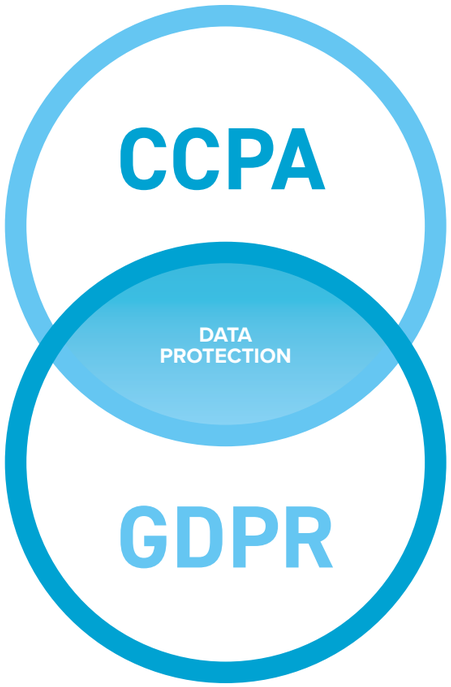
Additionally, to fall within the scope of the CCPA, your organisation must also meet one of the following three criteria:

- Receives, shares, buys or sells personal information of 50,000 consumers, households or devices per year (not necessarily in an exchange for remuneration);
- Gross revenue exceeding $25 Million; or
- Derives 50% or more of its annual revenue from selling consumer' personal information.

The CCPA also imposes obligations with respect to third parties and service providers. Your organisation therefore needs to identify and define its relationships with different parties and implement the necessary processes to comply with certain CCPA obligations such as opt-out sale rule.

Unlike the European General Data Protection Regulation (GDPR), the CCPA does not explicitly refer to "controller" and "processor" to distinguish the decision-making process by different entities with respect to personal data. However, the CCPA does define an organisation's "service provider" in similar manner to a "processor"; outlining that it is a legal entity that "processes information on behalf of a business". Many organisations that receive personal data from businesses subject to the CCPA will be considered 'service providers', although not those who themselves play a greater responsibility in determining the purposes and means of processing consumer's personal information (such as jointly on campaigns or projects).

In this scenario, the CCPA requires that service providers must be bound by a written agreement. Specifically, the contract must prohibit service providers from using consumer information disclosed to them for a purpose different than the one specified in the contractual terms.



B — WHAT IS A CONSUMER?

The CCPA applies to entities that collect personal information of "a consumer" which is defined as a natural person who is a California resident. The act gives a broad definition of California resident to include either:

- Individuals that are in California for other than a temporary or transitory purpose;
- Individuals domiciled in California but are currently out of the State for a temporary or transitory purpose.

One of the questions that arises is whether the definition of consumer covers employees. That is, does an organisation's employees, data fall under the CCPA definition of "consumer".

The recent amendment to CCPA (AB25 Bill) has modified the definition of personal information to exclude employees and provides a temporary exemption for employee data. Thus, until 1 January 2021 (a year after the CCPA enters into force), personal information collected from employees, job applicants, owners, directors, officers, medical staff and contractors of a business are exempt from most provisions of the CCPA (namely, those in relation to notice, access, deletion, opt-out, non-discrimination), as long as that information is used solely for employment purposes.

Additionally, the amendment provides that personal information acquired or used in a business-to-business (B2B) context, including for the purposes of products and services provided to businesses, will also be exempt from some rights (e.g. to notice, access, and deletion) until 2021.

However, organisations still have CCPA rights to consider in regard to their employees. This is the case of:

1. The exemption does not exclude the right of private action of employees in the event of a data breach.
2. Organisation still have the obligation to inform employees regarding the categories of information collected, used and disclosed by the employer, which should be included in their CCPA Privacy Notice.

After 1 January 2021, the one-year partial moratorium will end and the CCPA would become fully applicable to employees' personal data and personal information collected in a B2B context.

C — WHAT IS PERSONAL INFORMATION?

The CCPA provides an expansive definition of personal information covering any information that is “reasonably capable of being associated with or could reasonably be linked directly or indirectly with a particular consumer or household”.

The act offers a non-exhaustive list of what considers personal information. However, it is important to note that the information need to directly or indirectly connect to a particular consumer or household, otherwise it will not be subject to the CCPA.

The list includes, but not limited to:

- Identifiers such as real name, postal address, alias, unique personal identifier, IP address, device ID, email address, social security number, passport number, etc.
- Internet or other electronic network activity information, such as browsing history, search history, and information regarding a consumer’s interaction with an Internet Website, application, or advertisement.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric and geolocation information.
- Education; professional or employment-related information.

Additionally, organisations need to take into account that inferences drawn from any of above information to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, behaviour, attitude etc., are also considered personal information under the CCPA.

While the list may appear broadly extensive, the CCPA does exclude certain data from the scope of personal information. This is:

- De-identified or aggregated consumer information are entirely exempt from the Act.
- Publicly available information that is lawfully made available from federal, state or local government records are also excluded (companies cannot process this data for a different purpose).

Organisations which are subject to the below laws are excluded from the scope of the CCPA:

Non-profit organisations that do not operate for ‘profit and financial benefit’.

- Financial institutions that are regulated by the Gramm-Leach-Bliley Act (GLBA).
- Consumer reporting agencies that are regulated under the Fair Credit Reporting Act (FCRA).
- Health care providers that are regulated by the Health Insurance Portability and Accountability Act (HIPAA).

D — CONSUMER RIGHTS

The CCPA confers several privacy rights to Californian consumers which translates in subsequent obligations to your business. In order to address the new introduced consumer requests, your organisation needs to take significant steps to ensure CCPA compliance.

1. NOTICE RIGHTS:

The CCPA requires entities to provide consumers a general notice about the business's overall activities. Specifically, your business must inform at or before the point of collection what categories of personal data to be collected, and the proposes of its use, such as through a website or hard copy Privacy Notice (as appropriate).

Further notice will be required again in order to collect additional categories or use collected personal information for unrelated purposes.

Information collected through cookies, including a consumer's cookie ID, IP address and browsing history, will generally be considered personal information under the CCPA. Thus information on the cookies deployed must be provided in a Cookie Banner at the point of collection, whilst giving individuals the ability to opt-out to the cookies. However, unlike under the GDPR, opt-in tick boxes for specific types of cookies do not have to be implemented.

2. RIGHT TO ACCESS:

Californian consumers are entitled to request from a business the disclosure of information collected about them. Upon a verifiable consumer request, your business has the obligation to disclose to the specific consumer the following information pursuant to the request:

- ✓ The categories of personal information collected
- ✓ The sources from which the personal information is collected
- ✓ Business or commercial purposes of collecting or selling personal information
- ✓ The third parties with whom the data is shared
- ✓ Specific pieces of personal information the business holds about a consumer

Information on consumers must be provided as collected from the last 12 months (information collected previously does not need to be disclosed).

In addition to the above disclosure, if your organisation sells personal information or discloses it for business purposes, Californian consumers are also entitled to request the categories of personal information sold or disclosed.

After the receipt of a consumer's request, an organisation has 45 days to verify the request and deliver the information or inform the consumer that it will not take action. The information must be provided free of charge, in a readily usable format, and can be sent via an account, mail or electronically. However, the organisation may extend the time period to respond to any consumer request by up to 90 additional days where necessary, taking into account the complexity and number of the requests.

3. RIGHT TO OPT-OUT:

The CCPA provides consumers with the right to opt-out of the sale of their personal information to third parties. Consumers can exercise this right at any time by requiring a business not to sell their personal information.

Typically, companies must enable the opt-out of sale option by providing a "Do Not Sell My Personal Information" link through their website. Moreover, the organisation must also wait 12 months minimum before asking consumers to opt back in again.

Third parties must also give consumers explicit notice and an opportunity to opt out before re-selling personal information that the third party acquired from another business.

When the consumer is a minor, the CCPA provides for a right to opt-in to the sale of personal information. Your business must not sell the personal information of a minor unless you have an affirmative authorisation.

Your organisation may seek such authorisation from the parent or guardian if the minor is less than 13 years of age. In the case of consumers who are between 13 and 16 years of age, they can exercise the right to opt-in for sale by themselves.

It is important to note that whilst 'sale' is broader than simply covering providing information for financial remuneration, it does not include providing information to a service provider where the information is needed to be provided for a business purpose. Business purposes, among other examples, include performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider. As such, organisations will be able to provide information to suppliers, such as when using software as a service (SaaS) providers for customer relationship management (CRM) or Human Resources (HR) systems, without the need to provide an opt-out.

4. RIGHT TO REQUEST DELETION:

The CCPA also gives consumers the right to request from a business and its service providers the deletion of their personal information.

Like the right to erasure under the GDPR, this right is not an absolute right and it only applies in a limited number of situations. The CCPA specifically provides nine exceptions to the right to deletion, which covers situations such as:

- ✓ Information is necessary to detect security incidents;
- ✓ Complete a transaction for which the personal information has been collected
- ✓ Comply with a legal obligation;
- ✓ Exercise other rights such as free speech;
- ✓ Engage in scientific, historical, or statistical research in the public interest or;
- ✓ Information is necessary for internal uses reasonably aligned with the consumer's expectations.

5. NON-DISCRIMINATION RIGHT:

The CCPA prohibits discrimination against consumers for exercising certain rights under the law. The Act attempts to grant a right to equal service and generally prohibits organisations from practices such as:

- ✓ Denying goods or services to those consumers.
- ✓ Charging them different prices or rates, including through use of discounts or other benefits.
- ✓ Providing them with a different level or quality of service.
- ✓ Suggesting that they will receive a different level or quality of service.

The prohibition only applies where the consumer exercises specific rights, such as the right to access, to delete and opt-out of the sale of personal information. However, your business may offer financial incentives for the collection and the sale of personal information, but only with the consumer's opt-in consent and where the price or difference is related to the value of the consumer's data.

E — SECURITY OBLIGATIONS

Although the CCPA does not specifically regulate or require data security measures, it indirectly does so with respect to arrangements related to data breaches. It particular, it provides that a civil action can be launched for a data breach that results from a business' "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".

In relation to an understanding of what could constitute "reasonable security", the Californian Attorney General has endorsed the Center for Internet Security's Critical Security Controls. Chiefly, these include: to compile device/asset registers, maintain logs of security incidents that occur, ensure network security measures like firewalls and anti-malware are in place, carry out disk encryption with respect to personal information and ensure sufficient access controls to personal information are in place, among others. Organisations should consider implementing such measures on a risk basis.

F — FINES

For any violation of noncompliance with its provisions, the CCPA allows businesses a 30-day window to amend any violations (including of the rights and security obligations), so long as the organisation can prove they have been amended and that no more will occur. Otherwise, the Attorney General of California can institute a civil action. Organisations in breach of the CCPA's provisions might face penalties of up to $2,500 per violation and $2,500 per 'intentional' violation.

The CCPA also allows for the possibility for private rights of action (including class actions), which could lead to statutory damages of up to $750 per consumer per incident. However, the right to bring such an action is limited to situations where there is a breach of security, e.g. leading to a data breach. Namely, this occurs when non-encrypted or non- redacted personal information is subject to an unauthorised access and exfiltration, theft, or disclosure as a result of the business's violation of security obligations.

G — SUMMARY AND FUTURE ACTIONS

The CCPA is the most substantial privacy law so far passed in the United States and models the EU's GDPR in terms of the rights in brings to consumers and obligations imposed on businesses. The potential for heavy fines and class actions has instilled a shift in compliance with data protection in many businesses operating or collecting data from the state, and is likely to spark cases on the scope of its provisions, or prompt further data protection legislation within the USA. Whilst the majority of the obligations are process-orientated, the focus on responsibility for data breach notification and handling individual requests should lead organisations to prescribe the appropriate accountability within their governance frameworks.

As such, to ensure compliance by 1st January 2020, organisations should:

1. Conduct a data flow analysis to personal information within the scope of the CCPA;
2. Update or develop new policies and processes in line with the CCPA, such as their privacy notices, individual rights related policies and breach response processes
3. Conduct a due diligence assessment of third parties and service providers
4. Prepare their staff by providing training on the CCPA's provisions and their individual responsibilities

LONDON OFFICE

8 Fenchurch Place

London, EC3M 4AJ

Telephone: +44 (0)20 7090 1091

dataprotection@gemserv.com

IRELAND OFFICE

Fitzwilliam Hall Business Centre

Fitzwilliam Place, Dublin 2

Telephone: +353 (0) 1 669 4630

dataprotection@gemserv.com

Gemserv