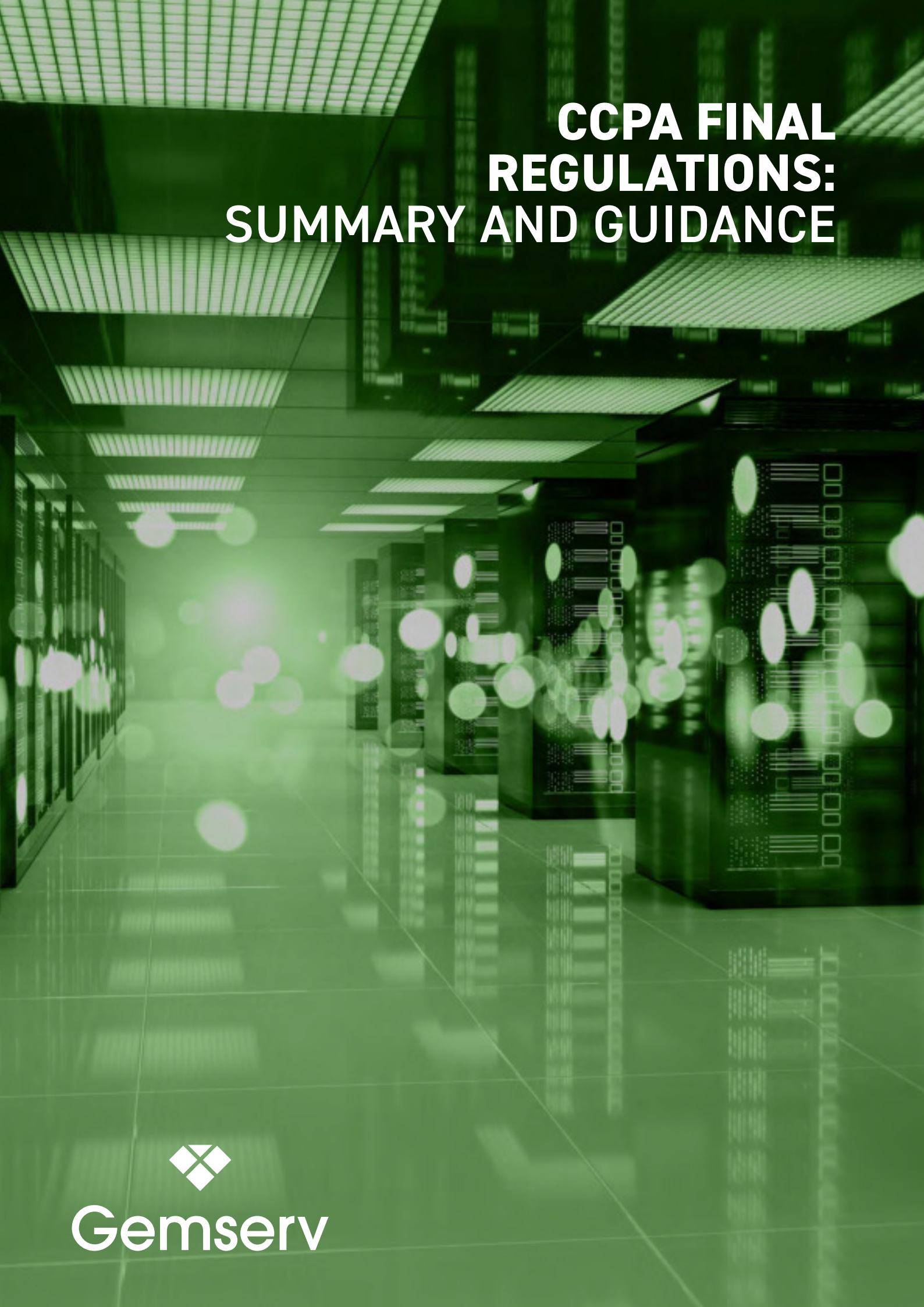

CCPA FINAL REGULATIONS: SUMMARY AND GUIDANCE

Gemserv

CCPA FINAL REGULATIONS: SUMMARY AND GUIDANCE

INTRODUCTION

The California Attorney General (AG) submitted, on 1st June 2020, the final version of the Regulations for the California Consumer Privacy Act (CCPA). The Regulations, which have been enforceable since 1st July 2020, govern compliance with the CCPA and aim to provide specific guidance regarding its practical implementation. A violation of these Regulations constitutes a violation of the CCPA, and it is subject to the same sanctions and remedies provided in the CCPA – meaning they are very important for organisations to remain aware of.

A chronological background of the Regulations can be summarised as follows:

- On 10th October 2019, the AG issued proposed regulations under the CCPA.
- On 7th February 2020, the AG released the first set of modifications made to proposed regulations.
- On 11th March 2020, the AG published the second set of modifications to the proposed regulations.
- The final version of the regulations were released on 1st June 2020.

Notably, the CCPA and the Regulations became enforceable on 1st July 2020 as the AG's office refused to postpone the enforcement deadline in light of the Covid-19 pandemic.

This guidance aims to clarify the relevant obligations that will impact business operations as well as provide technical and practical steps to address them.

CCPA FINAL REGULATIONS: SUMMARY AND GUIDANCE

NOTICE TO CONSUMERS

The Regulations provide a general overview of the required notices that businesses must disclose to consumers. These notices are aimed at providing information on how the business handles personal data. In specific situations separate notices must also set out:

- Notice at collection of personal information, for any business that collects information from a consumer (this should be provided at the point of collection).
- Notice of right to opt-out of sale of personal information, for a business that sells personal information (this is known as a Do Not Sell link, and can be provided through the website).
- Notice of financial incentive for a business that offers a financial incentive or price or service difference.
- Lastly and most importantly, the organisation's Privacy Policy.

The majority of these notices would typically be displayed on an organisation's website and are discussed in more detail below.

NOTICE AT COLLECTION OF PERSONAL INFORMATION

The purpose of the notice at collection is to provide consumers with timely notice, at or before the time point of collection, about the categories of personal information to be collected and the purposes for which the information will be used. In addition, a link to the business' "Do Not Sell My Personal Information" or "Do Not Sell My Info" notice and business's Privacy Policy must be included.

Typically, this would cover both an organisation's website Privacy Notice and Cookie Notice or Banner, as well as pop-up notices in place on mobile applications.

Where a business doesn't collect personal information directly from consumers, they do not have to give the notice at collection, as long as they do not sell consumers' personal information.

However, any company that doesn't collect personal information directly from consumers but 'sells' (i.e. exchanges in the course of business, as well as sells in the narrower sense) personal information to other parties as a data broker should register with the AG and provide its notice via a Privacy Policy link included with its registration.

NOTICE OF RIGHT TO OPT-OUT OF SALE OF PERSONAL INFORMATION

When a business sells the personal information of consumers, they must provide the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or the download or landing page of a mobile application.

'Sale' of personal information has a broad definition and includes providing information to third parties, unless such sharing is required for providing the service to the customer.

NOTICE OF FINANCIAL INCENTIVE

The Regulations also require notice or specification of a 'financial incentive'. This largely applies to organisations offering payments or cheaper products or services in return for the collection of customers' data – such as through loyalty programs where this information is collected.

The Regulations require businesses that offer a financial incentive to provide consumers with a notice that includes a summary of services offered: the material terms, including the categories of personal information involved and the value of the consumer's data; a mechanism to opt out of the incentive; and a statement of the consumer's right to withdraw.

PRIVACY POLICY

The purpose of the Privacy Policy is to provide the consumers with a comprehensive description of a business' online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information.

As such, in a similar manner to the GDPR Privacy Notice, this must be a more detailed description of the organisation's notice than the Notice at Collection. In practice, this will also apply through the organisation's website.

Gemserv

CCPA FINAL REGULATIONS: SUMMARY AND GUIDANCE

HANDLING CONSUMER REQUESTS

The Regulations provide details on the methods for submitting access and deletion requests, and how to respond to such requests.

METHODS FOR SUBMITTING REQUESTS TO KNOW AND REQUESTS TO DELETE

With respect to access and deletion requests, the following procedures should be put into place:

- Access Requests: Online businesses and those with a direct relationship with the consumer should provide an email address for submitting requests to know.
- Deletion Requests: Businesses should provide at least two methods for such requests – such as a toll-free phone number, a link or form available online through a business's website and a designated email address.

If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, a business can either treat the request as if it had been submitted in accordance with the business's designated manner, or provide the consumer with information on how to submit the request or remedy any deficiencies with the request.

RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE

The Regulations clarify that businesses have 10 business (not calendar) days to confirm these requests and 45 calendar (not business) days, from the date that the business receives the request, to respond. However, these periods can be extended if the business provides the consumer with notice and an explanation of the reason for the extension.

REQUESTS TO OPT-OUT

Businesses are required to provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive form accessible via a clear link entitled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business' website. Using a toll-free number is another method that could be employed.

Do Not Sell requests must also be respected by websites that deploy cookies. This typically included through an opt-out to variou s types of cookies (particularly third-party cookies) through a cookie banner.

The Regulations clarify that businesses typically have 15 business days to act on a "Do Not Sell" request from receipt. Businesses are also responsible for notifying third parties to which information has been sold of the opt-out request.

VERIFICATION OF REQUESTS

The Regulations require businesses to have a reasonable method to verify the identity of the person making the request. According to the Regulations, the development of a method must 'take into consideration the sensitivity and value of the information and the risk of fraud'.

Various methods could be used – for example, this may include requesting further information known to the business (i.e. to evidence address or purchase history) or, where a consumer has a password-protected account with the business, the business may use the authentication process for the account to verify the consumer's identity. However, if the business cannot verify the consumer within the 45-day time period, it may deny the request.

CCPA FINAL REGULATIONS: SUMMARY AND GUIDANCE

SPECIAL RULES REGARDING MINORS

Businesses that have actual knowledge of selling the personal information of minors are required to establish, document, and comply with a reasonable method to obtain a verifiable opt-in consent to the sale of personal information – either from minors if aged between 13 and 16, or from a parent if the minor is under the age of 13.

It is important to note that actual knowledge is not either defined in the CCPA or in the draft regulations. However, the CCPA explicitly states that a business which wilfully disregards the consumer's age has actual knowledge of the consumer's age. Thus, businesses that provide services that could be used or are likely to be used by minors should take active steps to determine the age of Californian residents, to avoid being considered to 'wilfully disregard the age' of minors.

This would include various website measures to:

- Determine the age of Californian residents (e.g. website or app users).
- Implement a process to reasonably ensure that the person providing consent for the sale of data is the child's parent or guardian.
- Document such consents in a secure manner.
- Include description of these processes in your privacy policy.

On a risk basis, organisations should recommend implementing tailored measures to determine a child's age, where a sale of data is to occur. This would depend on the business' typical services, users and/or clientele. This would include, for example:

- Business to business websites with no direct focus on minors (such as corporate estate agents): No age verification mechanism would necessarily be required.
- Websites obviously not targeting children (such as hardware stores): No age verification mechanism would necessarily be required.
- Websites which could collect children's data (e.g. sports goods stores): Age verification through a selection of a user's age (e.g. through a web tool or form) could be used, which would require opt-in consent for those under 16. Additionally, for those under the age of 13, this could be coupled with a requirement to collect parents' consent, such as a form signed by the parent or guardian.
- Websites targeted at children (e.g. some children's games websites or apps): An age verification mechanism should be used. In addition to the form, this could include a method to verify this (e.g. to enter the parent's credit card details) on sign-up, or requiring video verification of the parents' image (providing this image was not stored).

These methods would only be required if the business is involved in selling personal data.

Gemserv

EMPLOYEES:

Until January 2021, employees' personal data is excluded from most of the scope of the CCPA. Whilst the Regulations do not change this, two areas of compliance remain:

- Providing a notice at collection, and
- Maintaining reasonable security safeguards over employees' data.

For employees, a notice at the beginning of the onboarding process, such as with offer letters, might make sense. Additionally, the security measures are also relevant for companies' HR departments to implement, given that a private right of action can now be implemented by individuals suffering a data breach.

TRAINING AND RECORD-KEEPING:

Under the Regulations, businesses are required to ensure there are several other governance measures introduced within organisations, such as:

- Staff are aware and responsible for identifying and handling consumer requests (for example, through training and the appointment of relevant customer-facing or services staff).
- Staff maintain records of CCPA consumer requests (including opt-out requests) and how the business has responded, for at least 24 months.

Gemserv

Gemserv

LONDON

+44 (0)20 7090 1091

bd@gemserv.com

DUBLIN

+353 (0)1 669 4630

ireland@gemserv.com

CONTACT US TODAY, TO DISCOVER HOW WE CAN HELP YOU