CPRA: WHAT YOU NEED TO KNOW

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

This Report is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Report may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

Privacy Analysts

Alexis Kateifides, Nikolaos Papageorgiou,
Edidiong Udoh, Pranav Ananth, Angus Young,
Victoria Ashcroft

Image production credits
Cover photo: CGinspiration / Signature collection / istockphoto.com
Page 5: Pgiam / Signature collection / istockphoto.com
Page 6: libre de droit / Essentials collection / istockphoto.com
Page 7: choness / Essentials collection / istockphoto.com
Page 8-9: uschools / Signature collection / istockphoto.com

Published by OneTrust DataGuidance Limited, Dixon House, 1 Lloyd 's Avenue, London EC3N 3DS

Website **www.dataguidance.com**

Introduction

The California Privacy Rights Act of 2020 ('CPRA'), or Proposition 24, was passed with a 56% majority in the California General Election of 3 November 2020. The first version of the ballot initiative that became the CPRA was introduced in September 2019 by Alastair Mactaggart, Board Chair and Founder of the Californians for Consumer Privacy group and proponent of the California Consumer Privacy Act of 2018 ('CCPA'), which was passed by the California Legislature in June 2018.

The CPRA will enter into effect on 1 January 2023 and, with the exception of the right of access, it will apply to personal information collected by a business on or after 1 January 2022. In spite of the timeframe for compliance, there are several new requirements that organisations are already preparing for.

This document summarises the key changes the CPRA introduces including:

- sensitive personal information as a new category of personal information;
- additional and amended consumer data rights;
- expanded contractual requirements for service providers and third parties;
- new definitions for, among other key terms, 'sharing,' profiling,' and 'service providers;'
- the creation of a state privacy agency;
- new risk assessment and cybersecurity audit requirements;
- provisions on profiling; and
- extended exemptions.

CCPA CONNECT WORKSHOPS

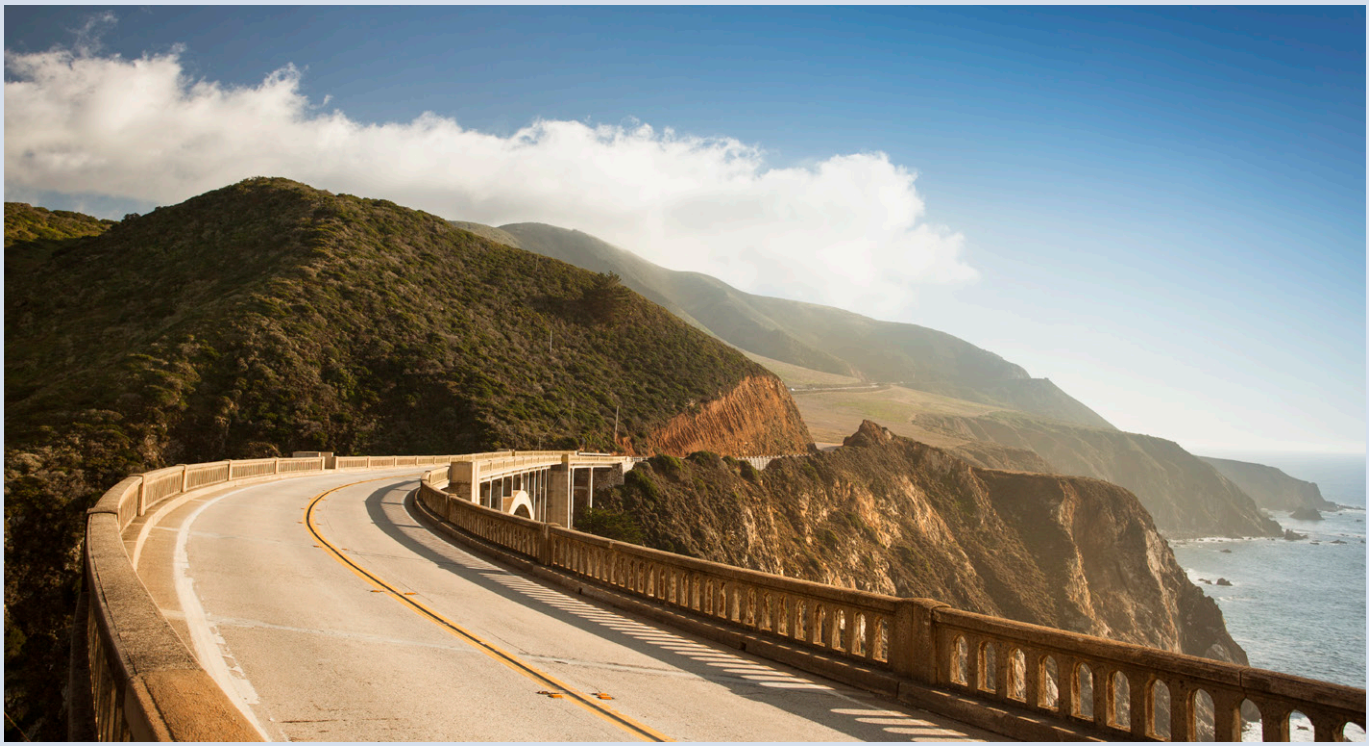
Join the conversation to hear what's next with the CCPA and CPRA and how to get your privacy program in order.

- *Free online events hosted globally*
- *Learn how to implement the CCPA & CPRA in practice*
- *Network with peers and earn CPE credits*

PrivacyConnect.com/CCPA-Connect-Workshops

REGISTER TODAY!

CCPA
CONNECT ONLINE
Workshops by OneTrust



Consumer rights

The CPRA will give consumers the right to request a company to update and correct inaccurate information a company may have about them and obliges the company to carry out the update or rectification.

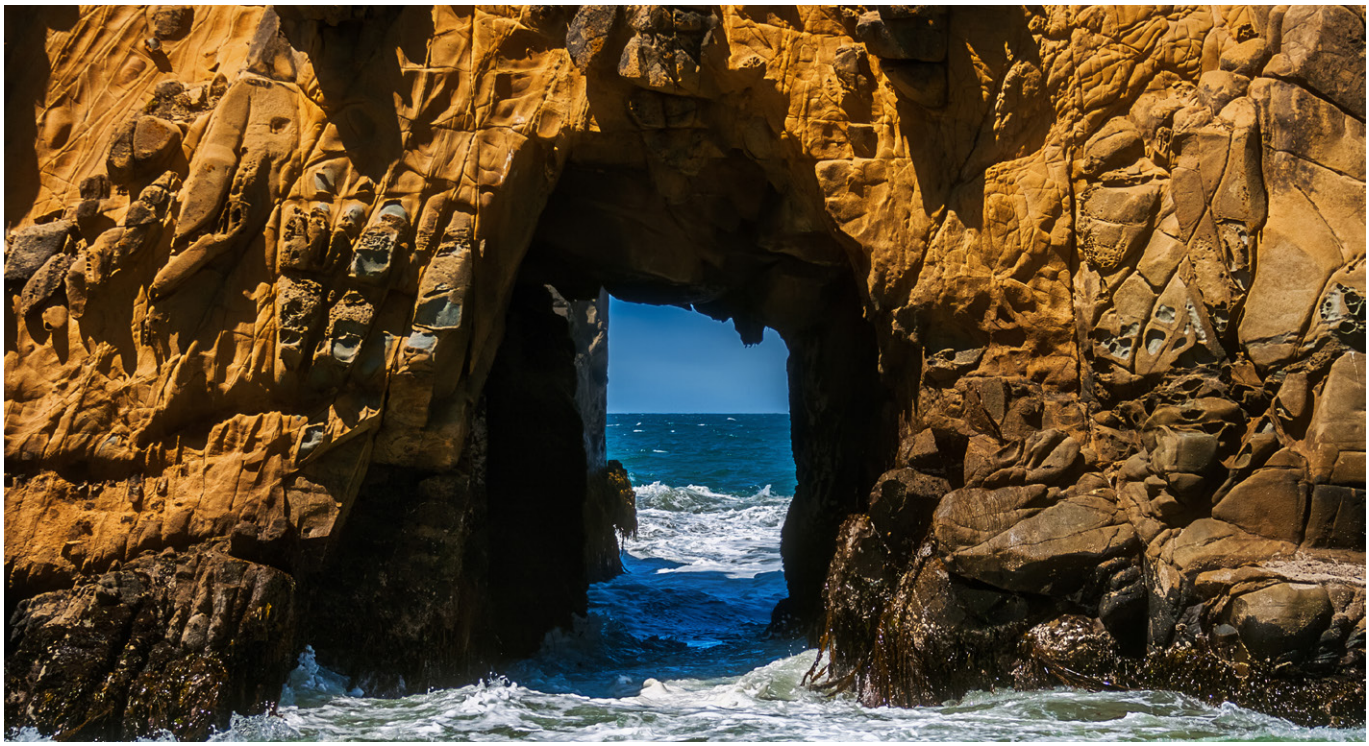
The CPRA will also extend the provisions for opt-out rules outlined in the CCPA. The CCPA's rules on opt out, as with most CCPA provisions, are based on the CCPA's definition of 'sale' which broadly includes acts of selling, renting, releasing, disclosing, disseminating, making available, and transferring personal information for monetary or other valuable consideration. This allows consumers to opt-out of the sale of their information to third parties.

The CPRA will expand the application of the opt-out rights to 'sharing' of information. The CPRA defines 'share,' 'shared,' or 'sharing' as 'sharing, 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 a third party for cross-context behavioural advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioural advertising for the benefit of a business in which no money is exchanged.'

Alongside the inclusion of the definition of sharing, the CPRA will limit the exemptions provided in the CCPA for the sale of information and revises the definition of sale to remove the inclusion of sharing to another business. There are certain exemptions to sharing including when the consumer has intentionally directed the business to intentionally disclose the personal information.

Thus, the CCPA expands opt-out rights to allow a consumer to opt-out of the sale and sharing of information to third parties.

With reference to opt-in rights, the CPRA will extend the right to opt-in to the sale or sharing of personal information for minors (consumers under 16 years old). If the consumer under 16 years old has declined to provide their information, the organisation is required to wait at least 12 months before approaching the consumer again for consent to sell or share their personal information.



Sensitive personal information

Similar to the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), the CPRA will introduce new requirements for 'sensitive personal information', which is a term that is not included in the CCPA.

'Sensitive personal information' is defined as '(1) personal information that reveals (A) a consumer's social security, driver's license, state identification card, or passport number; (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) a consumer's precise geolocation; (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; (F) a consumer's genetic data; and (2) (A) the processing of biometric information for the purpose of uniquely identifying a consumer; (B) personal information collected and analysed concerning a consumer's health; or (C) personal information collected and analysed concerning a consumer's sex life or sexual orientation.'

Categories and purposes of sensitive personal information that are collected or used by businesses must be communicated to consumers, at or before the point of collection. It will also be prohibited to use or collect additional sensitive information for purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without providing notice to consumers.

The CPRA will provide consumers with the right to limit the use and disclosure of sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services. In addition to the modified 'Do Not Sell or Share My Personal Information' links, businesses must provide a clear and conspicuous link on their internet homepage titled 'Limit the Use of My Sensitive Personal Information' that would enable a consumer, or a person authorised by the consumer, to exercise the aforementioned right. Nevertheless, a single link could be used by businesses to comply with this requirement, if such link easily allows a consumer to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

Service providers, contractors, and third parties

Contract requirements

The CPRA will significantly expand the contracting requirements for business that collect personal information in Section 4 by obliging all businesses that share personal information with a third party or that disclose personal information to a service provider or contractor for a business purpose to enter into an agreement with such, third party, service provider or contractor. The CPRA will also provide businesses with the authority to supervise compliance with the obligations outlined in the agreement by granting them the ability to 'take reasonable steps' to do so.

Contractors

Non-third parties are given a new definition under Section 15 of the CPRA as 'contractors,' which means a person who shares personal information with a business for a business purpose and pursuant to a written contract with the business. This definition is distinct from that of service providers under the CCPA. The agreement between a business and contractor must meet strict requirements including:

- use of personal information especially outside of the business purpose or relationship and combining the personal information provided;
- certifications outlining that the contractor is aware of the restrictions;
- granting permission for the ongoing monitoring of compliance of the contract by the business; and
- notification to the business when engaging any other party to assist in the processing of personal information.

New service provider definition and contractual obligations

The CPRA will modify the definition of service provider which now includes a requirement prohibiting services providers form selling or sharing the personal information that they have received from a business. Furthermore, service providers will be contractually prohibited form retaining, using, or disclosing the personal information they have received outside of the business relationship, as well as prohibited from combining the information with information the service provider receives or collects from another person. Similarly to the 'contractor' modifications, the contract between the business and service provider may, subject to agreement, permit the business to monitor the service providers compliance with the legislation with measures including ongoing manual reviews, and automated scans, and regular assessments, audits, or other technical and operational testing at least once every 12 months. Finally, the CPRA will add the obligation for a service provider to notify a business if it engages any person to assist in the processing of personal information for a business purpose on behalf of the business.

New state privacy agency

The CPRA will mandate the creation of a new state agency - the Consumer Protection Privacy Agency ('the Agency'), which would enforce the provisions of the CCPA and have the authority to take other actions against organisations for non-compliance. This new Agency would be the first of its kind in the US and would resemble the EU approach of supervisory authorities tailored towards privacy enforcements (data protection authorities) as well as shift powers from the California Attorney General.

Notably, under Section 24 of the CPRA the Agency is vested with full administrative, authority, and jurisdiction of the CCPA which would include modifications to the CCPA Regulations. The Agency would be governed by a five-membered board for eight-year terms including a Chair, with appointment powers being given to the AG, Senate Rules Committee, Speaker of the Assembly, and the Governor.

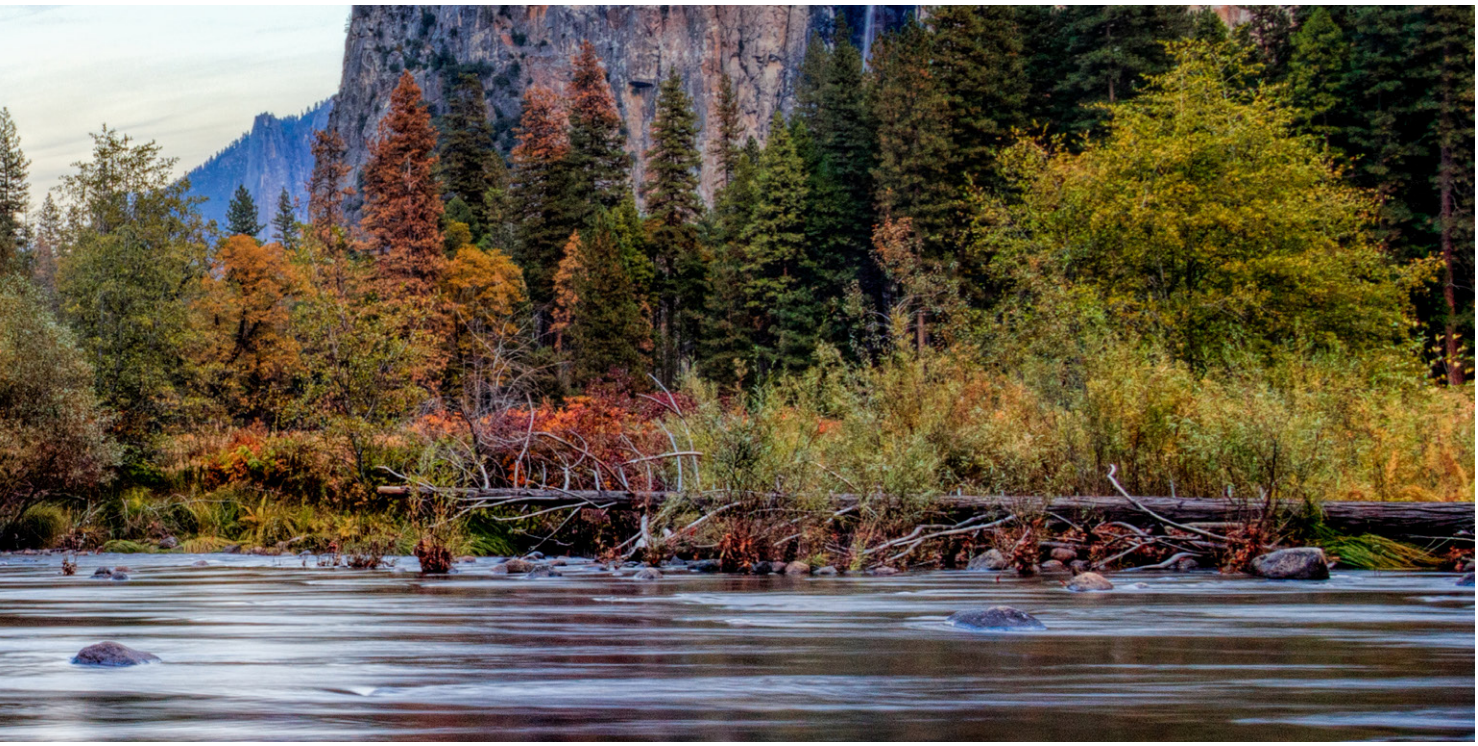
Under the CPRA, the Agency will be apportioned a $5 million budget during the fiscal year of 2020-2021, and the sum of $10 million during each subsequent fiscal year. There will be a six-month transition period whereby the Agency will provide the AG notice that it is prepared to assume rulemaking responsibilities. The deadline for this transition period is 1 July 2021. It is not clear what the role of the Agency will be during this transition period.

Risk assessments and cybersecurity audit requirements

The CPRA will direct the AG, and subsequently, the Agency to adopt regulations that mandate that businesses conduct a risk assessment with respect to their processing of personal information on a regular basis and submit these to the Agency. The CPRA outlines that the risk assessments should involve 'identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing.'

Although the concept of Data Protection Impact Assessments is already established, the provisions in the CPRA go further by requiring risk assessments be submitted to a regulatory authority.

Additionally, the CPRA will oblige business to perform a cybersecurity audit on an annual basis and establishes that the AG and subsequently the Agency issue regulations on the scope and processes of audits. The CPRA highlights during this process that size, complexity, and nature of



the processing should all be factors to consider in determining when processing may result in significant risk of harm to the individual.

Profiling

The CPRA will establish a new definition of profiling which means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person, and in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. The CPRA will also authorise the AG to issue regulations governing access and opt-out rights with respect to businesses' use of automated decision making, including profiling and requiring business' response to access requests to include meaning information about what was involved in these processes as well as a description of the likely outcome of the process in relation to the consumer.

Extended exemptions

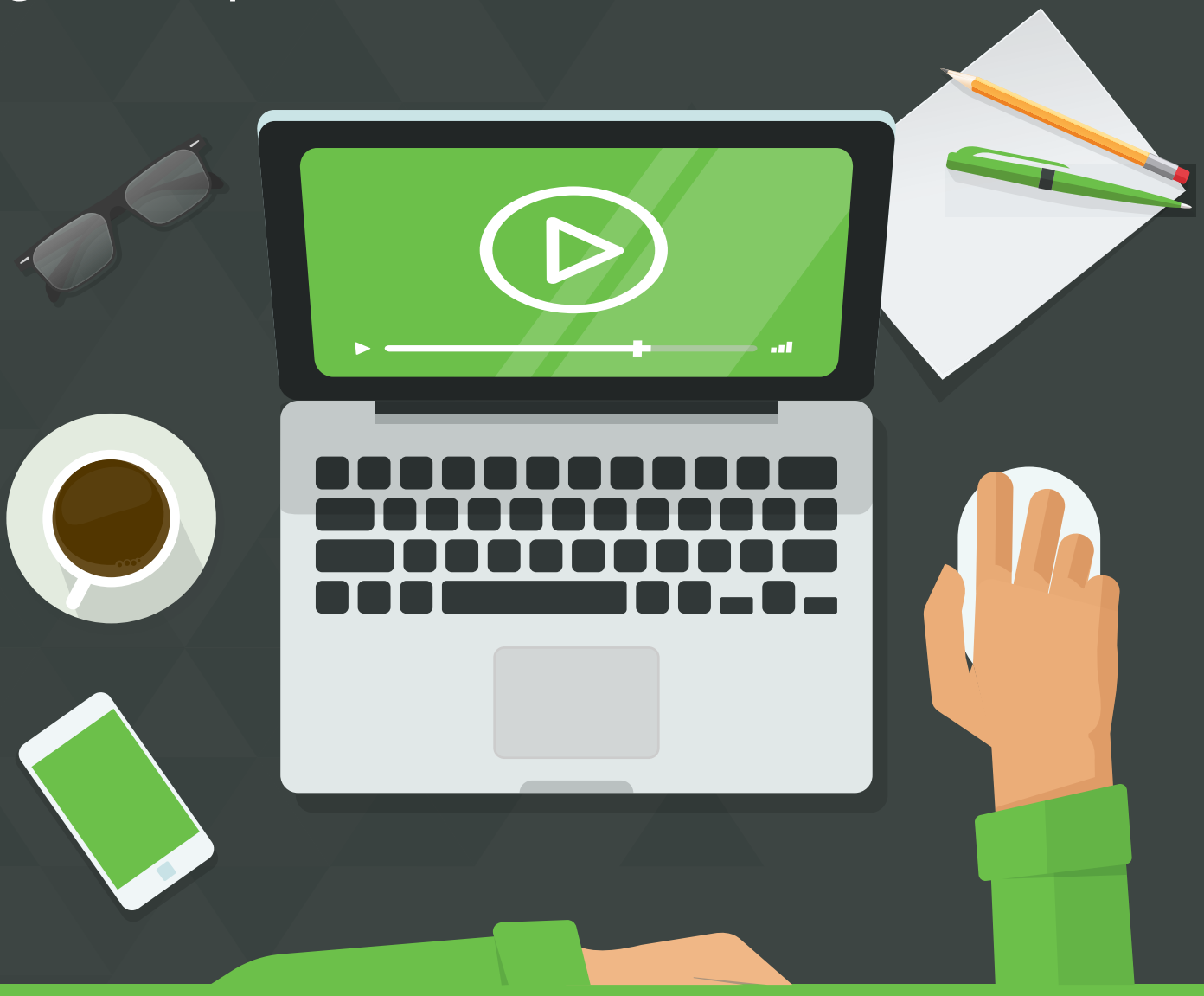
The CPRA will extend the exemptions provided under the CCPA for a moratorium on its regulations' application to organisations, extended until 2023 from the previously mandated expiry in 2022 in Assembly Bill 1281, with regards to collected employee data. The CPRA outlines that its regulations on business with regards to rules on the rights to deletion, correction, access, information and data minimisation, among others do not apply to organisations that collect data from a natural person in the course of the natural person acting as 'a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of that business.'

The moratorium on the application of the CPRA's rules applies to organisations until the 1 January 2023, following which the personal information collected in the employment context by organisations will fall under the purview of the previously mentioned regulations of the CPRA.

The CPRA will extend similar exemptions to personal information exchanged in business to business ('B2B') communications until 1 January 2023 as outlined in the CCPA. The CCPA provides this exemption to B2B communications where the consumer acts on behalf of the business and the information exchanged relates solely to the provision or receipt of a product or service to or from a business.

REQUEST A CPRA DEMO

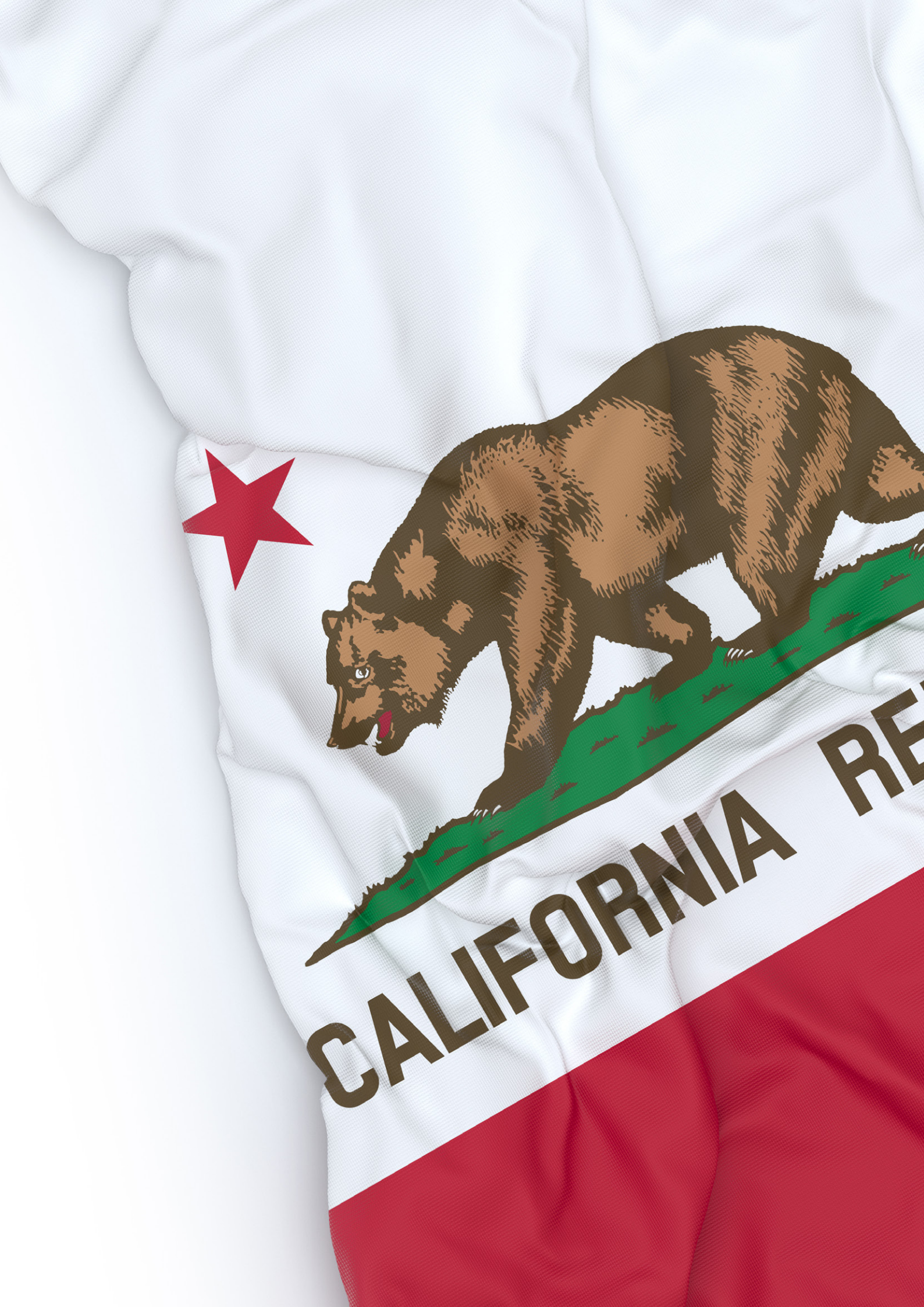
Is your business ready for the CPRA? Let one of our privacy solution experts take you on a deep dive tour of our suite of technology solutions for operationalizing and automating CPRA requirements.



OneTrust.com/CPRA-Request-Demo

REQUEST A DEMO TODAY!

OneTrust
PRIVACY, SECURITY & GOVERNANCE


CALIFORNIA RE