COMPLIANCE WITH THE CALIFORNIA CONSUMER PRIVACY ACT IN THE WORKPLACE: WHAT EMPLOYERS NEED TO KNOW

By Lydia F. de la Torre and Lauren Kitces[1]

I. INTRODUCTION

The California Consumer Privacy Act (CCPA) represents a quantum leap in consumer privacy and a major change in the regulatory framework applicable to companies doing business in California. The CCPA goes into effect on January 1, 2020, and imposes limits on the collection and sale of personal information by organizations that meet certain thresholds ('businesses') and provides certain individuals ('consumers') with four different rights and asserts an obligation on businesses: the right to opt-out of data sales (opt-in for minors), the right to delete, the right to know, the right to not be discriminated against for exercising any of the preceding rights and the obligation to inform. While the law contains certain limitations, at its core, it is based on the idea that consumers should have transparency regarding the use of their personal information, and control over aspects of its use.

The CCPA regulates the processing of data of 'consumers' and defines consumer to mean: (i) a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section reads on September 1, 2017, (ii) '*however identified, including by any unique identifier*'.[2] The term 'resident,' as defined in the law, includes (1) every individual who is in the State for a reason other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State and is outside the State for a temporary or transitory purpose.[3] Accordingly, the CCPA applies to employee data, contractor data, applicant data, and the data of company officers and directors who are residents of California.

The core of the CCPA is the broad definition of 'personal information.'[4] Due to this expansive definition, employers should assume that any information they might collect

---

1 Lydia de la Torre has extensive professional experience working on complex EU, US, and international privacy and data protection issues as outside counsel, in-house counsel, and consultant. She is currently Of Counsel at Squire Patton Boggs and an Adjunct Professor at Santa Clara University. Lauren Kitces has worked in several capacities addressing EU, US, and international privacy and data protection, and is currently an Associate at Squire Patton Boggs in Washington, D.C., in the Data Privacy and Cybersecurity Group. The views and opinions set forth herein are the personal views or opinions of the authors and do not necessarily reflect the views or opinions of the law firm with which they are associated.

2 Cal. Civ. Code Sec. 1798.140(g).

3 For an article providing a detailed explanation on what is a 'consumer' under the CCPA, see https://medium.com/golden-data/what-is-a-consumer-under-the-ccpa-fcdcfec776f0.

4 Under Cal. Civ. Code Sec. 1798.140(o)(1) "Personal Information" means 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.' There is pre-existing California law that aligns with this definition. In particular, Cal Civ. Sec. 1798.80 (e) defines personal information as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, […]."

and keep on any California resident who applies to work, works, or has worked for them is subject to the CCPA.

Guidance on the applicability of the CCPA in the workplace context will evolve as the Office of the Attorney General of California ('Attorney General') promulgates rules during 2020 and beyond. The CCPA requires rulemaking to be issued on specific topics, and also empowers the Attorney General to issue rules and provide guidance to address any aspect of the CCPA.[5] Public forums were held January through March of 2019. A notice of Proposed Regulatory Action ('Notice') is expected during the fourth quarter of 2019. After that, a new period for comments will open. Final rules are expected mid-2020. On October 2019 the Attorney General filed a notice of proposed rulemaking action[6] and published a proposed text for the CCPA regulations ("Proposed Rules").[7] The comment period on the Proposed Rules will be open through December 6, 2019.

This article provides a high-level overview of how the CCPA will impact an employer's privacy obligations under California law and identifies steps that employers should consider taking in order to minimize regulatory risks. The recommendations discussed in this article will not suffice to provide a complete picture of how any given individual organization will be impacted by the CCPA and does not constitute legal advice. It is essential for impacted employers to consult experienced privacy counsel in order to understand their specific exposure to the CCPA and plan accordingly.

II. EMPLOYEE PRIVACY IN CALIFORNIA PRIOR TO THE CCPA

In California, workers[8] have greater rights of privacy than in many other states. A worker's right of privacy begins with the California Constitution and is bolstered by various laws. In addition to the employee privacy regulations specified in the California Labor Code (cited below), employers have an obligation to comply with all general California privacy laws (i.e., laws that apply outside of the employment area such as the Fair Credit Reporting Act ('FCRA') and the Health Insurance Portability and Accountability Act ('HIPAA')).

Pre-CCPA privacy laws were typically conditioned on the existence of a 'reasonable expectation of privacy' and informing workers through handbooks, log-in scripts, and other means was generally sufficient to dismantle such expectations. Notwithstanding existing statutes, employers could, relatively easy, effectuate a waiver of California workers' privacy rights through unilateral notices disclosing data practices, which effectively meant workers could expect limited privacy in the workplace.

---

5 Cal. Civ. Code Sec. 1798.185.

6 Available online at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf

7 Available online at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf

8 For the purposes of this article, the term "worker" will be used to refer to *all* the following categories of individuals (provided that they are residents of the State of California): applicants (successful and unsuccessful), former applicants (successful and unsuccessful), workers (current and former), agency staff (current and former), casual staff residing in California (current and former), and independent contractors/consultants (current and former). Similarly, the term "employer" refers to an entity who has a worker providing their personal information.

Additionally, in certain circumstances California employers are expected (or legally required) to take actions that further limit workers' privacy rights. This includes, for example, taking affirmative steps to protect workers from harassment by co-workers, monitoring and enforcing compliance obligations under securities and financial laws, responding to government investigations, and producing evidence in discovery proceedings.

The pre-CCPA California laws specifically relevant to employee privacy include:

- **California Labor Code Section 96(k)**: Prohibiting employers from taking action against employees for lawful conduct that occurs away from the employer's premises during non-working hours.
- **California Labor Code Section 138.7(a)**: Regulating employer's access to worker compensation records.
- **California Labor Code Section 226:** Generally requiring employers to provide an employee's wage statement, but mandating that only the last four digits of an employee's social security number or identification number be printed on the statement.
- **California Labor Code Section 432.2**: Restricting the use of polygraphs on employees (similar restrictions exist at the federal level).
- **California Labor Code Section 432.7**: Including anti-discrimination provisions mandating that employers not consider juvenile criminal records as a factor in hiring, promoting, or terminating (subject to certain restrictions).
- **California Labor Code Section 435:** Generally prohibiting employers from causing an audio or video recording to be made of an employee in a restroom, locker room, or room designated for workers to change their clothes.
- **California Labor Code Section 980**: Generally prohibiting employers from demanding passwords and accessing social media accounts of employees and job applicants, except where it is reasonably believed to be relevant to an investigation of misconduct or violation of the law.
- **California Labor Code Section 1026:** Requiring employers to *'make reasonable efforts'* to safeguard the privacy of employees if the employee has enrolled in an alcohol or drug rehabilitation program.
- **California Labor Code Section 1198.5:** Granting employees the right to expect and receive copies of the personnel records that the employer maintains.
- **California Labor Code 6408(d):** Allowing access by employees or their representatives to accurate records of employee exposures to potentially toxic materials or harmful physical agents.
- **California Civil Code Section 52.7**: Prohibiting anyone from requiring, coercing, or compelling any other individual to have an identification device subcutaneously implanted, particularly by conditioning employment, employee benefits, or a promotion when consenting to the implant.

- **California Code of Civil Procedure Section 1985.6**: Mandating some specific rules that employers must observe when responding to subpoenas for the release of employee records.

- **California Fair Employment and Housing Act.**[9] Precluding employers from asking candidates about their age, national ancestry, religion, marital status, sexual orientation, or health conditions (subject to certain exceptions; similar restrictions exist at the federal level).

The CCPA expands workers' rights in various significant ways that are discussed in Section VIII below.

III. CCPA'S APPLICABILITY TO EMPLOYEE AND CONTRACTOR DATA AND THE WORKER DATA MORATORIUM

Following the enactment of the original version of CCPA in June 2018, the applicability of the CCPA to workers' data was the subject of debate. Reading the plain language of the CCPA, it was clear that the law regulated the personal information of consumers and defined 'consumer' to mean a resident of the State of California, which includes workers. However, a number of arguments were advanced to support the proposition that it was not the intent of the legislature to regulate workers' data.

The reasoning behind this argument centered mainly on the *'common understanding'* of the concept of a consumer as an individual who buys products or services for personal use. Following the passage of the CCPA, some organizations lobbied for a narrower definition of 'consumer' that would exclude both employees and contractors. Their efforts eventually resulted in the passage of a moratorium (hereinafter, the 'worker data moratorium') that partially carves out worker data until January 1, 2021. The worker data moratorium was enacted through consolidated bills Assembly Bill 25,[10] Assembly Bill 1355,[11] and Assembly Bill 1146.[12] Subsection (h) has been added to Cal. Civ. Code Sec. 1798.145, to state:

> *'(n) (1) This title shall not apply to any of the following:*
>
> > *(A) Personal information that is collected by a business about 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 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*

9 Cal. Gov. Code Sec 12900-12996

10 Assembly Bill 25. Introduced by Assembly Member Chau (Coauthors: Senators Dodd and Hertzberg) on December 03, 2018, and available online at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml? bill_id=201920200AB25.

11 Assembly Bill 1355. Introduced by Assembly Member Chau on February 22, 2019, and available online at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1355.

12 Assembly Bill 1146. Introduced by Assembly Member Berman on February 21, 2019, and available online at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1146.

to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.'

The worker data moratorium settles the question of whether the CCPA regulates worker data: it clearly does. The exclusions in the moratorium are limited, as discussed more fully in sections IV and V below. Absent further legislative developments, after 2020 all CCPA provisions will be fully applicable to worker data.

IV. WHICH EMPLOYERS ARE REGULATED BY THE CCPA?

The CCPA only applies to employers that qualify as a 'business.'[13] A 'business' can either qualify directly (if it meets certain requirements) or indirectly (if it controls or is controlled by a business that qualifies directly and operates under the 'common branding').

- To qualify directly, an entity must: operate for-profit, directly or indirectly collect data of *'consumers'*, *'alone, or jointly with others'*, determine *'the purposes and means of the processing'* (i.e. be a controller),[14] be established (*'do business'*[15] in the State of California), and meet one of three thresholds: (1) annual sales of $25M or more; (2) buy, sell, or share for *'commercial purposes'*[16] 50,000 or more personal records; or (3) derive 50% or more of its annual revenue from selling *'personal information'*.

- To qualify indirectly, an entity must be a parent or a subsidiary of an entity that qualifies directly and share common branding with that entity. A 'business' that qualifies 'indirectly' need not be established in California (i.e. do businesses[17] in the State), operate for profit, or determine *'the purposes and means'* of the processing.[18]

Even employers that operate mainly in the business-to-business space will be deemed a 'business' as to their workers' data if they meet the thresholds described above. Nonprofit entities will be exempt from compliance provided that they do not belong to a business group that qualifies directly as a 'business' and operate under the same brand. The Attorney General may issue further guidance or rules clarifying the applicability of the CCPA that could possibly exempt certain entities from compliance.

V. WHAT WORKER DATA IS REGULATED BY THE CCPA?

The broad definition of personal information means that employers should assume that any information they might collect and keep on any California resident who applies

---

13 Cal. Civ. Code Sec. 1798.140(c)(1)&(2)

14 For an explanation of the concept of controller under EU law, see https://medium.com/golden-data/what-is-a-controller-afd99a8ebd0a

15 For an explanation of the concept of 'doing business' in California, see https://medium.com/golden-data/what-is-a-doing-business-in-california-under-ccpa-90ddd964115b

16 For an explanation of what constitutes 'commercial purposes' under CCPA, see https://medium.com/golden-data/what-are-business-and-commercial-purposes-under-ccpa-ed45728aad0

17 *Id* at 13.

18 For an article on the general concept of 'controller,' see https://medium.com/golden-data/what-is-a-controller-afd99a8ebd0a.

to work, works, or has worked for them is subject to the CCPA. This would include the data of:

- applicants (successful and unsuccessful) who are residents of California;
- former applicants who are residents of California (successful and unsuccessful);
- employees who are residents of California (current and former);
- agency staff residing in California (current and former);
- casual staff residing in California (current and former);
- contract staff (i.e., independent contractors or consultants) residing in California (current and former);
- individuals acting as owners, directors, or officers who reside in California (current or former); and/or
- medical staff residing in California (current and former).

Since employers are generally required to identify the residency of their employees in order to comply with tax retention obligations, identifying whether an employee is a resident of California should not be problematic. However, identifying residency for staff hired through agencies, contractors, directors, and officers may require the employer to take additional steps.

Since the applicability of the CCPA is not limited to information collected or kept in electronic form,[19] employers also should assume that the CCPA applies to information kept in paper form.

Examples of personal information covered by the CCPA

Types of personal information relevant to the employment context include: traditional identifiers (e.g. name, address, phone number, social security number, email address etc.), job applicant information, benefits information, professional or employment-related information (e.g. compensation, performance reviews), geolocation information, internet activity (e.g. browsing history, interactions with websites), medical information not covered by HIPAA and/or characteristics of protected classifications and disabilities, employee emails, records of internal investigations, whistleblower hotline complaints, records of disciplinary proceedings, and even CCTV footage to the extent it captures images of workers.

Examples of personal information likely to be covered by the CCPA include:

- details of a worker's salary and bank account details held on an organization's computer system;

19 Cal. Civ Code Sec. 1798.175.

- an e-mail or handwritten notes about an incident involving a named employee in a supervisor's notebook which contains information on the employee, whether or not there is an intention to put that information in that worker's computerized personnel file;
- an individual worker's personnel file where the documents are filed chronologically by date, whether there is an index to the documents at the front of the file or not;
- an individual employee's personnel file where at least some of the documents are filed behind sub-dividers with headings such as: application details, leave record, and performance reviews;
- a set of leave cards where each worker has an individual card regardless of whether the cards are kept in alphabetical order or not; and
- a set of completed application forms, filed in alphabetical order within a file of application forms for a particular vacancy.

Examples of information unlikely to be covered by the CCPA include:

- information on the entire workforce's salary structure, given by grade, where individuals are not named and are not otherwise identifiable;
- a report on the comparative success of different recruitment campaigns where no details regarding individuals are held; or
- a report on the results of 'exit interviews' where all responses are anonymized and where the results are impossible to trace back to individuals.

VI. CCPA EXCLUSIONS RELEVANT TO WORKER'S DATA

In addition to the worker data moratorium, several of the CCPA exclusions are particularly relevant in the employment context:

- **Health Data exclusion:** Personal information regulated by HIPAA and related federal and state health information laws is excluded from the CCPA.[20]
- **Fair Credit Reporting Act exclusion:** The FCRA generally preempts state level legislation, but the CCPA actually contains an explicit carve out for data subject to the FCRA (for example, employers obtaining consumer reports on prospective employees need not modify their practices to account for the CCPA).[21]
- **B2B communications moratorium:** There is a limited moratorium on CCPA's applicability to certain B2B information, which will expire on January 1, 2021. The exception is limited to communications and transactions occurring solely within the context of due diligence and situations where a product or service is provided or received. Under this moratorium, businesses will not have

20 Cal. Civ. Code Sec. 1798.145(c).

21 Cal. Civ. Code Sec. 1798.145(d).

to comply with their obligation to inform, provide access, or honor deletion requests with respect to B2B information. Businesses will still have to comply with opt-out and non-discrimination obligations.[22]

- **General exclusions:** The obligations imposed by the CCPA on employers do not apply to the extent that they could restrain the business's ability to: comply with federal, state, or local laws; comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law; or exercise or defend legal claims.[23]

- **De-identified or aggregate data (as defined under CCPA):** De-identified and aggregate data are both excluded from the applicability of the CCPA. But the CCPA does define both categories in a narrow way. Therefore, employers wishing to rely on this carve out should carefully analyze if the data in question meets the CCPA de-identification or aggregation standards.[24]

CCPA and the California Workers Compensation System

The California Workers Compensation System (CWCS) is not expressly excluded from applicability of the CCPA. The Attorney General has broad authority to identify additional exemptions and a number of organizations have specifically requested that the CWCS be exempted.[25]

Given the fact that CWCS is a Constitutional mandate (under Section 4 of Article XIV of the California Constitution) and is already regulated under California law (see section II above), it would be logical for the Attorney General to include a full or partial CCPA exemption in updates to the Proposed Rules or in future rule-making. However, the Proposed Rules do not include any exemption for CWCS.

VII. HOW SHOULD EMPLOYERS PREPARE FOR CCPA COMPLIANCE?

The CCPA will take effect on January 1, 2020. With regards to workers' personal information however, given the worker data moratorium, the CCPA will go into effect in two phases:

- From January 1, 2020 to December 31, 2020 the CCPA will apply to worker data subject to the partial exclusion provided by the worker data moratorium.

---

22 Cal. Civ. Code Sec. 1798.145 (n).

23 Cal. Civ. Code Sec. 1798.145(a).

24 Cal. Civ. Code Sec. 1798.145(a)(5).

25 *See, for example*, comments filed by Kammerer and Company Inc., on behalf of American Association of Payers, Administrators and Networks (AAPAN); Anthem Workers' Compensation; Coventry; MEDEX; Healthcare Risk and Insurance Management Society (RIMS)–California; and Small Business California, at page 344 of the combined PDF, including all written submissions available online at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

- From January 1, 2021 onward all of the CCPA provisions will apply to worker data absent further legislative developments.

Accordingly, it is advisable for employers to organize their CCPA compliance efforts into two different phases: Pre-2020 and post-2020.

A. What Should Employers Do On Or Before January 1, 2020?

The worker data moratorium will significantly reduce certain qualifying employers' CCPA obligations, depending on their existing data management practices. The carve-out is generous, but not unlimited. Specifically, the following limitations apply to the worker data moratorium:

- **Context of the worker role limitation:** In general, the use of worker personal information by employers outside "*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 a contractor of that 'business'* is not covered by the carve out.[26]

- **Emergency contact information:** Personal information collected for emergency contact purposes is only excluded if '*collected and used solely within the context of having an emergency contact on file.*'[27]

- **Benefits administration data:** Personal information necessary to retain and administer benefits is only carved out '*to the extent that the personal information is collected and used solely within the context of administering those benefits.*'[28] That said, if such information were subject to HIPAA, it would be deemed permanently excluded from the CCPA as described in section VI above and remain subject exclusively to HIPAA instead.

Therefore, employers should bear in mind that using worker data for any purposes other than employment related purposes will likely result in the data falling outside of the scope of the worker data moratorium. Where worker data falls outside of the worker data moratorium, all the rights and obligations identified in Section VII.B. will apply on January 1, 2020.

In addition, the worker data moratorium is subject to two significant carve outs:

- **The right to be informed:** The worker data moratorium requires employers to provide certain information to workers. Employers may not undertake any new information collection protocols or use the already collected information without providing notice.[29] If the employer activities qualify for the worker data moratorium, a narrow reading of the relevant provisions leads to the conclusion that the notice obligations may be modest (i.e. limited to information surrounding

---

26 Cal. Civ. Code Sec. 1798.145 (h)(1)(A).

27 Cal. Civ. Code Sec. 1798.145 (h)(1)(B).

28 Cal. Civ. Code Sec. 1798.145 (h)(1)(C).

29 Cal. Civ. Code Sec. 1798.100 (b).

what worker data is collected and how it is used).[30] However, providing a full CCPA notice on or before January 1, 2020 constitutes best practice.

- **Data breach litigation risks:** The CCPA creates a private right of action in the event of a data breach resulting from the failure to put in place reasonable security measures.[31] Remedies include injunctive relief and damages of no less than $100 and no more than $750 per consumer per incident. The worker data moratorium does not limit the applicability of this right. Employers' litigation risks in the event of a breach involving worker data will therefore increase significantly as of January 1, 2020.

It is important to note that the private right of action under the CCPA[32] is not predicated on the definition of personal information under CCPA, but on the more narrow definition of personal data under subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 of the California Civil Code.

Steps employers should take prior to January 1, 2020

- **Understand if you qualify for the worker data moratorium:** As above, using (or allowing others to use) worker data for any purposes other than employment related purposes will likely result in the data falling outside of the scope of the worker data moratorium. Accordingly, the first step that employers should take is to identify any situations in which they use or allow others to use worker data for non-employment purposes. This may include, for example, worker's contract details shared with third-party benefit providers where the contract permits the third party to use the details to market additional services to the worker. If the data falls outside of the worker data moratorium, all the rights and obligations identified in Section VII.B. apply as of January 1, 2020.

- **Know your data:** As the CCPA requirements are predicated on how employers collect, use, and share worker data, employers intending to comply with the CCPA should take stock of their data practices. This is typically achieved through a data inventory and mapping exercise. Employing a standardized taxonomy to catalog the data and, where possible, tagging the data is advisable as it can greatly facilitate compliance with the rights to know and delete. Once employers collect the necessary information, they can accurately assess their risks, identify their legal obligations, detect security issues, and isolate any problematic practices or operational inefficiencies. The discovery process should reveal what personal information employers hold about their workers, in which systems it is being held, and how that information flows within and outside of the employer's technology ecosystem. To the extent that worker data has already been mapped for compliance with other laws (such as the European Union's General Data Protection Regulation (GDPR)), employers may able to leverage the information they already have on hand.

---

30 Cal. Civ. Code Sec. 1798.100(b).

31 Cal. Civ. Code Sec. 1798.150.

32 *Id.*

- **Adjust practices or provide full rights:** Employers that wish to take full advantage of the worker data moratorium, but may be sharing or using worker data outside of the context of employment, should adjust their practices before January 1, 2020. Employers that prefer not to adjust their practices should prepare to provide full CCPA rights to workers regarding data that falls outside of the scope of the worker data moratorium as of January 1, 2020.

- **Identify the notification process:** Employers should consider the need for different notification processes depending on whether the workers are applicants, employees, contractors, casual workers, officers, etc. The process selected should ensure that such individuals receive the notice. If the employer maintains an intranet page, providing notice through that portal may suffice for workers who have access to it. If data for applicants is collected through an online portal, posting notice on that portal may suffice to notify applicants. In any event, workers should have access to the notice and be informed of where it can be found.[33]

- **Draft the language:** As discussed above, if the employer moratorium applies, a narrow reading of the relevant provisions supports taking the position that employers need only identify the categories of personal information and the purposes (business or commercial) for which the categories are used. However, the best practice would be to provide a full CCPA privacy notice as described in Section VII.B.

- **Notify:** Before January 1, 2020, employers should notify workers of their privacy practices.

- **Reasonable security:** As of January 1, 2020, workers will have the right to bring a private right of action against any employer that suffers a breach of security, caused by a lack of reasonable security, which leads to: unauthorized access and exfiltration, theft, or disclosure of non-encrypted or non-redacted personal information of workers. Reviewing and strengthening existing security practices and implementing state-of-the-art controls during 2019 and beyond will be an important factor in reducing reputation, regulatory, and litigation risks. In particular, employers should explore how technical measures such as redaction or encryption could limit their potential liability.

- **Review record retention policies and practices:** Employers should evaluate their record retention (destruction/deletion) policies and practices to determine what periods are legally mandated and how long each category of personal information is in fact retained under current practices. A good record retention policy should identify the legal obligations that apply to maintaining worker's records and, if records must be kept for other reasons, the basis for the retention time frames. If the employer does not have a written record retention policy and schedules, or if the policy and schedules have not been updated recently, it is

33 CCPA notification requirements are somewhat misaligned with an employer/worker scenario. For a detailed discussion on what may or may not constitute sufficient notification under CCPA, see Section VII.B.

advisable to address these shortcomings as soon as possible. Where there are no legal obligations to retain, employers should delete data as soon as it is no longer needed. Limiting retention to the extent possible during 2019 will significantly lessen the burden of compliance with the full CCPA rights in 2020 and beyond while simultaneously mitigating risks in the event of security breaches.

- **Review contracts with vendors:** Although the CCPA does not require that specific language be added to contracts with vendors that process worker data, it provides certain safe harbors for organizations that do. In addition, in order to operationalize the CCPA rights (such as the rights to know or delete), employers will need the cooperation of certain vendors. An initial step is to inventory all contracts in which the employer shares worker personal information with a vendor.

- **Training:** Although the obligation to provide training in regard to worker personal information is delayed by the worker data moratorium until January 1, 2021, it would be prudent for employers to take the steps necessary to ensure that their human resources staff is sufficiently knowledgeable to be able to respond to questions related to the applicability of the worker data moratorium during 2020.

B. What Should Employers Do Starting January 1, 2021?

New bills aimed at either expanding or extending the applicability of the worker data moratorium will likely be introduced during the 2021 legislative session in California. However, because it is uncertain whether such efforts will succeed, employers should prepare for full CCPA applicability to workers' data as of January 1, 2021.

Employers must understand the full scope of the individual CCPA rights that will be afforded to workers in 2021 and be ready to implement the systems and processes that will be necessary to respond to situations where workers exercise those rights.

VIII. WORKERS' RIGHTS UNDER THE CCPA

Once the CCPA is fully applicable to worker data (i.e., once the worker data moratorium has expired or the employer uses or plans to use worker data outside the context of their employment), workers will be entitled to exercise all their rights under the Act. These rights may raise particular issues in the employer/worker context, which will need to be carefully assessed. This section provides a high-level description of the workers' rights and identifies some of the issues they will raise in the workplace context.

In order to enable workers to effectuate their rights, the CCPA imposes certain related obligations on employers such as verifying the requesting worker's identity (authentication), promptly acting on worker requests, and updating privacy notices to include, among other things, a description of the California workers' rights, the purpose(s) of personal information collection, and identification of the categories of personal information that are 'sold' (as broadly defined by CCPA), collected, or disclosed for 'business purposes'.

In certain situations, the CCPA authorizes employers to decline to respond to workers' requests submitted under CCPA. Specifically:

1. an employer can assert that it is not subject to the CCPA (i.e. the employer is not a 'business' under CCPA);[34]

2. an employer can assert that the worker is not protected by the CCPA (e.g., the worker is no longer a resident in the State of California);[35]

3. the worker's request to exercise a right is not verifiable (i.e., the employer cannot properly authenticate the requesting individual);

4. the request would require the employer to re-identify data or otherwise link information that is not maintained in a manner that is considered to be personal information.[36]

A. Right to Know

Under the CCPA, workers will have the right to know, which provides them with access to their personal information and includes a limited right to data portability.[37] At a high level, workers will be able to (i) obtain confirmation of whether their personal information is being sold and other supplementary information, and (ii) access personal information about them that is being held by the employer.

This right must be exercised through a 'verifiable consumer request'. The employer must properly verify the requesting worker's identity, and then comply with the request within 45 days of receipt (an extension is possible if 'reasonably necessary,' but the worker must be notified). An employer may provide personal information to a worker at any time, but is not required to provide it more than twice in a twelve-month period.

The specifics of the access rights provided under the CCPA are complex but, at a high-level, they can be broken down into two categories:

- **Confirmation of data sold and general information:** For employers that 'sell' or disclose personal information for a 'business purpose,'[38] workers have the right to request the disclosure of the categories of personal information collected and sold, and the categories of third parties to whom the data is sold. In addition, workers have the right to be informed about the categories of personal information disclosed for a 'business purpose.'[39] Once the requesting worker's identity is verified, the employer must create two separate lists: one including the categories and sources of personal information sold and a separate list of categories and sources of personal information disclosed for 'business purposes.'[40]

---

34 For more details, see Section IV above.

35 For more details, see Section V above.

36 Cal. Civ. Code Section 1798.145(i).

37 Cal. Civ. Code Section 1798.100.

38 For an explanation of what 'business purpose' means under CCPA, see https://medium.com/golden-data/purposes-for-processing-under-ccpa-3e329ddd218

39 Cal. Civ. Code Sections 1798.115(a)&(c) and 130(a)(5)(c).

40 Cal. Civ. Code Section 1798.130(a)(4).

In addition, employers must disclose the categories of third parties with whom the information is shared.

- **Specific pieces of information:** Finally, workers will have a right to request the disclosure of the specific pieces of personal information 'collected' (as broadly defined under CCPA) about them in the preceding twelve months. The information may be delivered by mail or electronically. If provided electronically, the information must be in a portable and, to the extent technically feasible, readily usable format that allows the worker to transmit this information to another entity without hindrance (this requirement is typically referred to as the CCPA's right to 'data portability'.)[41]

Under the pre-CCPA privacy laws, employment records are deemed confidential in California and disclosure is restricted absent a subpoena and notice. Workers have certain access rights under various California laws other than the CCPA but, until the CCPA, the right was limited to specific categories of data. In particular, a right to inspect exists for the following employment records: payroll records (Lab. Code § 226); documents signed during employment (Lab. Code § 432); personnel records including records related to performance or a grievance (Lab. Code § 1198.5); and OSHA records for employee exposures to potentially toxic materials (Lab. Code § 6408(d)). Failure to comply with these inspection rights gives rise to statutory damages. For example, Labor Code 226 requires employers to allow inspection of payroll records within 21 days after a request is made, or else the employee is entitled to $750 in statutory damages.

The CCPA's right to know significantly expands the right of access under existing California law and raises specific questions in the workplace context. For example, under the CCPA, workers can request access to confidential performance reviews or internal correspondence about themselves, with no exception for confidential information. Employers can generally deny access, however, if providing the information requested could *'adversely affect the rights and freedoms of other consumers.'*[39] It may sometimes be challenging for an employer to know when the right to know might adversely affect someone else's rights but, at a minimum, redactions to eliminate references to other identifiable individuals that may be referenced in the information that must be disclosed will be necessary. The Attorney General has broad authority to issue rules providing clarity on this point but the Proposed Rules do not address it.

B. Obligation to Inform

At a high level, the CCPA obligation to inform[42] requires, among others, the following elements to be included in the privacy notice:

- Information surrounding what worker data is collected and how it is used.[43]

41 Cal. Civ. Code Sections 1798.100(d) and 1798.130(a)(2).

42 Cal. Civ. Code Sections 1798.130(a)(5) and 1798.100(b).

43 *Ibid.*

- Details on what worker data is both sold and disclosed and if selling and/or disclosing is not happening, then a statement reflecting this.[44]
- A description of the worker's rights, and appropriate contact methods to effectuate those rights.[45]
- Information on the right to opt-out of the sale of worker data, and a link to the *'DO NOT SELL MY PERSONAL INFORMATION'* button that is required to be made available on the homepage.[46]

Disclosure of privacy practices to workers though policies and other documents is not new in California. For example, notices and policies are currently used to disclose the use of workplace monitoring in order to diminish expectations of privacy as mentioned in Section II above. The California courts have reinforced the importance of employers maintaining and widely publicizing notice with respect to the use of technology in the workplace and have upheld an employer's right to monitor its workers' computer use so long as there is a policy in place that makes it clear that workers have no expectation of privacy in regards to data transmitted on company systems.

The CCPA and Proposed Rules impose detailed notification obligations on employers and requires the notices to include very specific language. Although the CCPA requires a detailed breakdown describing data practices, it does not directly restrict the ability of employers to monitor workers. However, to the extent that such monitoring involves the use of vendors that gain access to worker personal information, the CCPA could impose indirect restrictions on monitoring. This is due to the fact that the CCPA imposes restrictions on data transfers to third parties that are deemed to constitute a 'sale' (see Section VII.B.1.c.).

C. Right to 'Opt-Out' ('Opt-In' for Minors Under 16) of Data 'Sales'

The CCPA gives workers, or their authorized agents, the ability to direct employers to stop selling[47] their personal information to third parties[48]. For children under 16 (whose personal information may be collected in certain workplace environments, such as a minor working at the local movie theater), employers must not sell personal information unless or until the employer obtains authorization from a parent or guardian (if less than 13) or the minor (when 13 or older) before selling.

Once the requesting worker's identity (or the identity of its representative and the authorization to represent) is verified, the employer must stop selling personal information to third parties. The worker may subsequently provide express authorization for the sale of personal information. The employer must respect the worker's decision to opt-out for

---

44 Cal. Civ. Code Sections 1798.115(c)(1), 115(c)(2), and 130(a)(5)(C).

45 Cal. Civ. Code Section 1798.130(a)(5)(A).

46 Cal. Civ. Code Section 1798.135(a)(1)-(a)(2).

47 For an explanation of what constitutes a data sale, see https://medium.com/golden-data/what-is-a-sale-under-ccpa-b27fbe8a527.

48 Cal. Civ. Code Section 1798.120.

at least 12 months before requesting a new authorization from the worker to the sale.[49] The personal information collected in connection with the exercise of the right to opt-out may be used by the employer for complying with the request, even where such use could be otherwise considered a sale under the CCPA.[50]

Most employers do not actively sell their workers' data in the usual sense of the word. Given the broad definition of sale under the CCPA, however, sharing agreements that may not be perceived by the employer as data sales could fall under the scope of the right to opt-out. Employers should carefully review all transfers of worker data to vendors to ensure that they do not fall within the CCPA definition of 'sale' in order to determine whether they are required to offer an opt-out to their workers.

D. Right to Delete Data

The CCPA gives workers a general right to request their employer delete personal information that the employer collected from them.[51]

The obligation to comply with a deletion request is subject to various exceptions, including the right of the employer to keep data if necessary to meet a legal obligation or for the employer's internal use if otherwise lawful and compatible with the context in which the information was provided by the worker. The majority of employee or applicant data will likely fall under one of these two exceptions.

In addition, employers can generally deny a deletion request if erasing the information could *'adversely affect the rights and freedoms of other consumers.'*[52] It sometimes may be challenging for an employer to know when erasing worker's personal information might adversely affect someone else's rights. Consider, for example, situations when a worker requests deletion of disciplinary records that are outside of a statutorily prescribed retention period, but potentially relevant to future situations involving allegations of workplace harassment. The Attorney General has broad authority to issue rules and guidelines providing clarity on this point, but the Proposed Rules do not address it.

E. Right to Not Be Discriminated Against for Exercising a Right Under CCPA

The CCPA generally prohibits discrimination against a worker for exercising his or her rights under the CCPA[53]. The examples of discrimination provided under the CCPA are not geared toward the employment context and include situations such as denying goods or services, charging different prices or rates for goods or services, or providing a different level or quality of goods or services. CCPA permits charging a different price, rate, level or quality of service in certain circumstances and also allows providing incentives in specific cases.

---

49 Cal. Civ. Code Section 1798.135(a)(5).

50 *Ibid.*

51 Cal. Civ. Code Section 1798.105.

52 Cal. Civ. Code Section 1798.145(j).

53 Cal. Civ. Code Section 1798.125.

Although the CCPA anti-discrimination provision does not specifically refer to firing, declining promotion opportunities, or offering different terms of employment to workers who exercise their rights under the CCPA, any of those actions could be considered discriminatory if found to constitute retaliation against workers for exercising their CCPA rights. One of the open questions that will have to be addressed is which party bears the burden of proof in these situations. If any disciplinary decision taken after a worker exercises a CCPA right is to be conceived as retaliatory in nature absent proof to the contrary provided by the employer, the liability risk could be significant. The Proposed Rules do not address these issues.

IX. OTHER CONSIDERATIONS

In addition to requiring employers to respond to California workers' requests and give effect to their CCPA rights, the CCPA includes several additional obligations that apply to employers subject to limited exceptions summarized below.

A. CCPA Training

Employers are required to train and educate workers that handle CCPA consumer (including worker) inquiries about rights and related obligations prescribed by the CCPA[54]. In the context of employment, employers must ensure that their human resources team is knowledgeable about worker rights under the CCPA, and can assist workers wishing to exercise their rights under the law.[55]

Although the obligation to provide training in regard to worker personal information is delayed by the worker data moratorium until January 1, 2021, it would be prudent for employers at least to take the steps necessary to ensure that their human resources staff is sufficiently knowledgeable to be able to respond to questions related to the applicability of the worker data moratorium during 2020.

B. Designate Methods for Consumers to Assert Their Rights

An employer must implement two or more designated methods for workers to submit requests for information, including a toll-free telephone number (subject to certain exceptions not relevant in the employment arena).[56]

C. Contracts Containing Specific Criteria to Protect Privacy and Limit Exposure

There is no specific requirement in the CCPA to execute contracts. However, CCPA provides certain benefits where contracts containing specific language are executed[57] (e.g. in order to qualify as a 'service provider' as defined in the CCPA a written contract is required and, absent such contract, the sharing of personal data could potentially be

54 Cal. Civ. Code Section 1798.130(a)(6).

55 Cal. Civ. Code Sections 1798.130(a)(1) and 1798.140(i).

56 Cal. Civ. Code Sections 1798.130(a).

57 *See, e.g.,* Cal. Civ. Code Section 1798.140(i) and (w).

deemed a sale subject to the right to opt-out/opt-in[58]). Careful drafting and signing of CCPA compliant contracts may have the additional benefit of reducing the liability of the employer in the event of lack of compliance by a vendor.

Because specialized CCPA compliant contract terms may be beneficial, employers should evaluate whether to enter into them, as well as examine the particular language to be included carefully.

D. Employee Responsibility and the CCPA

Although the CCPA does not directly impose any obligation on workers, it is important to remember that organizations are made up of individuals. Therefore, workers—as well as employers—must take responsibility if full compliance with the CCPA is to be achieved. For example:

- Managers are responsible for the type of personal information they collect and how they use it.
- No one at any level should disclose personal information outside the organization's procedures, or use personal information in company records for their own purposes.
- Anyone disclosing personal information without the authority of the organization may expose the organization to liability, unless there is a legal justification (for example, under 'whistle-blowing' legislation). Individual liability may also be an issue.

As a result, employers should consider developing and implementing policies that provide clear guidance to employees as to their responsibilities to support compliance with the CCPA in the specific context of their particular companies' lines of business.

X. RE-THINKING WORKER PRIVACY POST-CCPA: MOVING TOWARDS A BEST PRACTICES CODE

The CCPA represents a quantum leap for worker privacy in California, and employers should not put off self-examination of practices in light of the new rules. Moving forward, privacy compliance should become an integral part of employment practices. Focusing on fostering a culture in which respect for private life, security, and confidentiality of personal information are the norm is the key.

The Attorney General has not issued guidance on best practices for privacy compliance in the workplace context. However, the UK Information Commissioner's Office (the 'ICO') has published a useful Employment Practices Code[59] that outlines a number of recommendations. Although not modeled after the CCPA, the code is a useful resource to benchmark practices for employers wanting to understand the privacy issues and options in the workplace context.

---

58 Cal. Civ. Code Section 1798.140(v); 1798.140(t)(2)(C).

59 The ICO Employment Practices Code is available online at https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf.

Some instructive recommendations contained in the ICO's Code, as adapted to California practice, are as follows:

1. Identify the person or group within the organization responsible for ensuring that the organization's employment policies and procedures comply with the CCPA and put in place a mechanism for checking that procedures are followed in practice.

2. Ensure that business areas and individual line managers who process worker information understand their own responsibility for privacy compliance and, if necessary, amend working practices and procedures in the light of this.

3. Assess what categories of personal information about workers are collected and maintained and who is responsible for it.

4. Eliminate the collection of personal information that is irrelevant or excessive to the employment relationship. If sensitive data is collected, ensure that it is strictly necessary and subject to appropriate access controls and security measures.

5. Ensure that all workers are aware that they can be liable if they knowingly or recklessly disclose personal information outside their employer's policies and procedures. Make serious breaches of data protection rules a disciplinary matter.

6. Consult workers, and/or trade unions or other representatives, about the development and implementation of employment practices and procedures that involve the processing of personal information about workers.

XI. CONCLUSION

The CCPA applies to worker data and will require employers to strike a balance between the legitimate privacy expectations of workers and their own interests in deciding how best to run their businesses, within the confines of the law. The legal requirements related to the applicability of CCPA in the context of employment will continue to evolve. The public comment period on the Proposed Regulations is open through December 6, 2019, and there is no definite date on which final regulations will be issued. The Attorney General is able to continue to issue proposed changes to the regulations once the final version is released, and further legislative developments are also possible.

In the meantime, employers should take immediate steps to reduce risks and embed privacy compliance in their employment policies and practices. Fostering a culture in which respect for private life, security, and confidentiality of personal information is the norm is key for organizations wishing to adapt to the stringent demands of the CCPA.