Engage PEO Client Alert:
The California Consumer Privacy Act of 2018 (CCPA)

On January 1, 2020, the expansive California Consumer Privacy Act of 2018 (CCPA) takes effect. The CCPA will impose security safeguards on covered business in an effort to protect the privacy of personal information of California residents. Without question, the CCPA will impact businesses in and outside of California.

CCPA-Covered Businesses

The CCPA applies to a business that meets the following criteria:

1. Is a for-profit entity;
2. Does business in California;
3. Collects personal information of California residents (or on behalf of which such information is collected);
4. Alone (or jointly with others) determines the purposes and means of the processing of such personal information; **and**
5. Satisfies at least one of the following thresholds:
    a. Annual gross revenue in excess of $25 million;
    b. Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more customers; or
    c. Derives at least 50 % of its annual revenues from selling consumers' personal information.

The term "business" also includes a business that controls or is controlled by a business that meets the CCPA test **and** shares common branding with that business. The terms "control" and "controlled" mean:

1. Ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a covered business;
2. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
3. Power to exercise a controlling influence over the management of a company.

Please note that the CCPA distinguishes between a "service provider" (which processes personal information on behalf of a business) and a "third party" (which sells personal information).

Further, the CCPA applies to the following:

- Identifiers (e.g., real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers);
- Any of the categories of personal information described in the California Customer Records statute (Cal. Civ. Code § 1798.80(e));
- Information regarding an individual's membership in a protected class under California and federal law;

- Commercial information (e.g., company services or products purchased);
- Biometric information (e.g., time clocks);
- Internet or other electronic network activity information (e.g., browsing history);
- Geolocation data (e.g., information collected by tracking devices/applications);
- Audio, electronic, visual, thermal olfactory or similar information;
- Professional or employment-related information;
- Non-public education information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99); and
- Inferences drawn from any of the categories of information described above.

The CCPA does <u>not</u> apply to:

- Publicly available information;
- Where compliance would violate the California evidentiary privilege;
- Personal information subject to HIPAA or California's Confidentiality of Medical Information Act;
- The sale of personal information to or from a consumer reporting agency if the information is to be reported in, or used to generate, a consumer report, and use of that information is limited by the federal Fair Credit Reporting Act;
- Personal information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act and implementing regulations, or the California Financial Information Privacy Act; and
- Personal information collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act of 1994.

Limited Exemption for HR Data

Until January 1, 2021, the following HR Data is exempt from the CCPA:

1. **Human Resources Data**: Personal information 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 to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business;
2. **Emergency Contact Data:** Personal information 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; and
3. **Third-Party Benefits Data:** Personal information 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.

Although employers are exempt from most portions of the CCPA until January 2021, beginning January 1, 2020, CCPA-covered employers must still comply with the CCPA and issue CCPA privacy notices explaining the categories of personal information collected and the purposes for which the business collected the personal information at the time of or before the collection of such information. Additionally, employees will have a private right of action (described below) to file individual and class action lawsuits for data breaches involving the employee's personal information.

CCPA Rights Effective January 1, 2021

Beginning January 1, 2021, covered businesses must make available at least two mechanisms for consumers to submit requests regarding their rights under the CCPA. At minimum, a covered business must provide consumers with a toll-free telephone number to submit consumer requests. If a covered business maintains an internet website, the business makes the website available to consumers to submit requests for information pursuant to the CCPA. Covered businesses that operate exclusively online and have a direct relationship with consumers from whom they collect personal information are only required to provide consumers with an email address to submit CCPA requests regarding their personal information.

Additionally, effective January 1, 2021, California consumers/workers will have the following CCPA rights:

- To request disclosure of the personal information the CCPA-covered business has collected;
- To know what personal information is being sold or disclosed and to whom;
- To request and receive a copy of the covered personal information in a readily useable format;
- To request that the business delete their personal information;
- To opt-out and opt-in to the sale of their personal information; and
- To be free from discrimination for exercising their CCPA rights.

Penalties for Violations

The CCPA grants the Attorney General authority to enforce the law by filing:

- Actions for ***intentional*** violations of the CCPA for civil penalties for up to $7,500 per violation; and
- Actions for ***unintentional*** violations of the CCPA for civil penalties for up to $2,500 per violation.

Before filing enforcement actions, the Attorney General must give a business 30 days to cure any alleged violation(s).

Additionally, the CCPA created a limited private right of action. If consumers' nonencrypted and nonredacted "personal information," as defined by a separate statutory section,[1] is subject to an

[1] California Civil Code section 1798.81.5 defines "personal information" to include the following: "(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number or California identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information. (B) A username or email address in combination with a password or security question and answer that would permit access to an online account. (2) 'Medical information' means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.
(3) 'Health insurance information' means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. (4) 'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." Cal. Civ. Code § 1798.81.5(d)(1).

unauthorized access and exfiltration, theft, or disclosure as a result of a covered business's violation of the duty to implement and maintain reasonable security procedures nature of the information to protect the personal information, consumers may file a lawsuit (on an individual or class action basis) for the following statutory remedies:

- $100 to $750 per incident or actual damages – whichever is greater;
- Injunctive or declaratory relief; and
- Other relief the court "deems proper."

Checklist to Prepare for 2020:

✓ **Determine whether your business is covered by the CCPA;**

If your business is subject to the CCPA:

- ✓ Identify and inventory (and continue to track) all data that may be considered personal information per the CCPA;
- ✓ Identify and inventory (and continue to track) all data any third party and/or service provider has which may be considered personal information for your employees and consumers per the CCPA (including benefits providers, insurance companies, payroll companies, staffing vendors, etc.);
- ✓ Revise service/vendor agreements to include language that requires third parties and service providers to comply with the CCPA;
- ✓ Confirm employee data is reasonably secured to avoid data breaches;
- ✓ Create or update your business's privacy policy to describe employees' CCPA rights as well as their emergency contacts and dependents;
- ✓ At the time of or before the collection of personal information, issue CCPA notices to the following describing (1) the categories of personal information to be collected; and (2) the purpose(s) for which the categories of personal information will be used:
    - job applicants,
    - employees,
    - owners,
    - directors,
    - officers,
    - medical staff member, and
    - independent contractors.

CCPA Notices should also include the following:

- ✓ If the business sells personal information, a link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info," or in the case of offline notices, the web address for the webpage to which it links; and
    - ✓ A link to the business's privacy policy, or in the case of offline notices, the web address of the business's privacy policy.