The California Consumer Privacy Act

Avature

V1

What You Need to Know About CCPA

The California Consumer Privacy Act ("CCPA"), which has been in effect since January 1, 2020, is a wide-ranging data privacy law that grants new rights to California residents relating to their Personal Information (defined below):

- The **right to know** what Personal Information is collected, used, shared, or sold, both as to the categories and specific pieces of Personal Information.
- The **right to delete** Personal Information held by businesses and by extension, a business's service provider.
- The **right to opt-out of sale** of Personal Information.
- The **right to non-discrimination** in terms of price or service when a consumer exercises a privacy right under the CCPA.

Furthermore, the CCPA increases the penalties and fines on violations of existing laws as a way to hold businesses more accountable for privacy breaches and securing consumers' Personal Information.

In order to be in compliance, companies will need to:

- Be familiar with the CCPA requirements,
- Establish business processes that are designed to support these requirements and consumer rights,
- Process Personal Information legally and ensure their service providers implement reasonable security practices and comply with consumer requests.

Recruiting and marketing programs, which depend on collecting and using Personal Information, face one of the biggest challenges. It is important to remember that the CCPA definition of Personal Information is broad. The CCPA defines "Personal Information" as 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. In other words, anything that could relate to a person or household should be considered Personal Information for CCPA purposes.

Penalties

The California Attorney General may bring actions for civil penalties from $2,500 for a non-intentional violation to $7,500 for an intentional violation of the CCPA per record involved. The CCPA also contains a private right of action that

consumers can bring under certain circumstances if a business experiences a data breach due to a violation of its duty to implement and maintain reasonable security procedures and practices.

At first glance, these can sound like a relatively small fines in relation to other privacy penalties, however, these will be applied per record so can add up quickly. For example, a company that has made a violation affecting 50,000 consumers could be looking at the following fines:

Non-intentional violation

= $2,500 x 50,000

= **$125 million**

Intentional violation

= $7,500 x 50,000

= **$375 million**

Impacted Parties

Consumers: The CCPA covers California consumers, which are natural people who are California residents. Your prospects, candidates and employees are the consumers. It is their Personal Information that is collected and processed when they are kept in a talent pool, considered for a position, hired and/or their performance and capacities considered for a raise or a promotion, etc. While the CCPA exempts Personal Information collected about employees and applicants from some CCPA rights for the first year the law is in effect, your employees and applicants still have some rights, including the right to know the categories of Personal Information collected about them and the purposes for which the information will be used.

Businesses: The businesses that are subject to the CCPA are for-profit businesses that do business in California, collect the Personal Information of consumers, and satisfy one or more of the following three criteria:

- Have annual gross revenues over $25 million,
- Annually receive, sell, or share Personal Information about more than 50,000 or more California consumers or households or 50,000 devices; or,
- Derive 50% or more of their annual revenue from selling Personal Information of consumers.

Service Providers: A service provider is a company that processes Personal Information on behalf of a business client, and is not permitted to retain, use, or disclose that Personal Information for any purpose other than for performing the contracted services. This is consistent with the way in which Avature operates. As a service provider, Avature does not have any direct responsibilities under the CCPA. However, our platform maintains and protects your candidates' Personal Information and our consultants are ready, willing and able to assist our customers in configuring the Avature platform to comply with CCPA processes.

So How Can We Help?

Can recruiting programs comply with CCPA and remain effective?

The short answer is yes.

Avature has been helping customers comply with other similar privacy laws for years, including the EU General Data Protection Regulation (GDPR).

Our customers — which include large and small enterprises, all the major global consulting companies, many of the largest banks and manufacturers in the US that do business in California, etc. — have developed competitive recruiting programs that operate effectively throughout the world and meet the data regulations.

If you still haven't done anything to comply with CCPA, you need to move quickly because, as with many of our non-EU customers or those not already subject to stringent privacy laws like the GDPR, you may need to make significant changes to the way you document and notify consumers about the way you collect and process Personal Information.

The good news is that Avature can be configured to support CCPA-compliant recruitment marketing programs.

Avature's security and privacy controls meet the highest standards and are ISO 27001 and SOC 2 certified. Our controls have passed multiple onsite audits and penetration tests.

Avature, Your Information Processing Partner

Leveraging our fundamental focus on configuration, we have invested in technical functionality specifically designed to support privacy laws. Our system is highly configurable, and you can determine how to process information in the manner that is legally compliant.

We have also assisted customers in their response to government inquiries relating to individual citizens' privacy complaints and supported customers in their successful resolution of complaints.

Support & Security Measures

Our main responsibilities as a service provider are to provide for the confidentiality, integrity, availability, and resilience of your information. Behind the user interface, we implement technical and organizational security measures such as:

- Firewall, encryption, and other technologies to protect the information,

- Separation of processing for different customers and their different purposes,
- Role segregation so that only Avature employees who need to access your data are able to view it.

Features

The Avature platform is designed for configurability. So when compliance regulations change, our technology can keep pace.

Specific to CCPA, our solutions offer different features to help you achieve compliance:

- Customizable opt-in/out or double opt-in workflows that automate the consent process and regularly re-evaluate candidate consent, including to opt out of selling Personal Information.
- Automated purging or deletion of data at intervals determined by you, including easy options for individuals to delete Personal Information.
- Encryption that keeps confidential data accessible/editable on a need-to-know basis.
- Configurable security settings for your users in accordance with your security needs.
- Full audit journal to trace interactions with candidates, including consents, notices, updates, and changes.
- Unsubscribe links in emails sent through Avature so candidates can choose to opt-out.
- Links to notice forms to manage and keep track of individuals' views of notices with timestamp.
- Quick linking to privacy policies, compliance with privacy law, and data protection resources.
- Avature's online documentation (Help & News), available from within your instance, describes in detail how all of our features work.

With CCPA now in effect, if your legal counsel advises you to reconfigure your instance, please contact your sales representative and our consultants will support any reconfiguration according to your instructions. For more information, contact your sales representative or email: **sales@avature.net.**

"At Avature we are used to working with large, complex, multinational businesses so this is not the first time we have assisted our customers in complying with new privacy regulations. As we inevitably see more regulation changes across different markets, I am confident that our customizable platform -focused on privacy by design- enables customers to adapt to these changes while ensuring their recruiting programs remain as competitive as ever."

Beatriz Quintana
Chief Privacy Officer

---

* While Avature offers functionalities to support compliant processes, we are not a law firm and do not provide legal advice. We have, however, worked directly with the legal departments of major organizations and their recruiting teams to implement compliant recruiting programs. Avature's consultants have supported the implementation of many recruiting programs for customers subject to CCPA, following their requirements in accordance with CCPA and other applicable privacy laws. We strongly recommend you consult with your legal counsel to decide upon compliance processes.