CASSIE
SYRENIS

Staffing Agencies

California Consumer Privacy Act (CCPA):

How staffing agencies can turn compliance into a strategic advantage

Contents

Introduction

On January 1st 2020 the California Consumer Privacy Act (CCPA) came into effect and changed the face of consumer data in the state of California forever. However, with Amendment AB25's January 2021 deadline entering the scene, many staffing agencies have been left confused about when they need to become compliant and how the laws will affect their how affect their day-to-day business operations.

With the CCPA aiming to bridge the gaps in other American legislative law, and AB25 acting as a temporary measure, it's hard to know when to start implementing long term solutions. With complex and conflicting advice surfacing, we wanted to simplify what the CCPA, and amendment AB25, means for staffing agencies.

"Of the organizations that have acheived compliance, 92% said they gained competitive advantage."

Capgemini (2019)
Championing Data Protection and Privacy Report

This paper aims to give you clarity on:

01 The unique challenges staffing agencies face when dealing with personal data

02 The kinds of personal data staffing agencies hold and the impact of the new legislation

03 What the term 'consumers' means and how it affects data in relation to employees

04 The dangers of not being compliant and how it can impact your business

05 The differences between GDPR and CCPA

06 How to stay compliant in an ever-changing landscape

07 How to turn compliance into a strategic advantage

Armed with this knowledge, you'll confidently be able to prepare for the new legislation, and varying deadlines. Informed by our years of expertise in the data privacy industry, this paper will assist your organization to navigate the complex landscape of CCPA.

Does CCPA apply to your staffing agency?

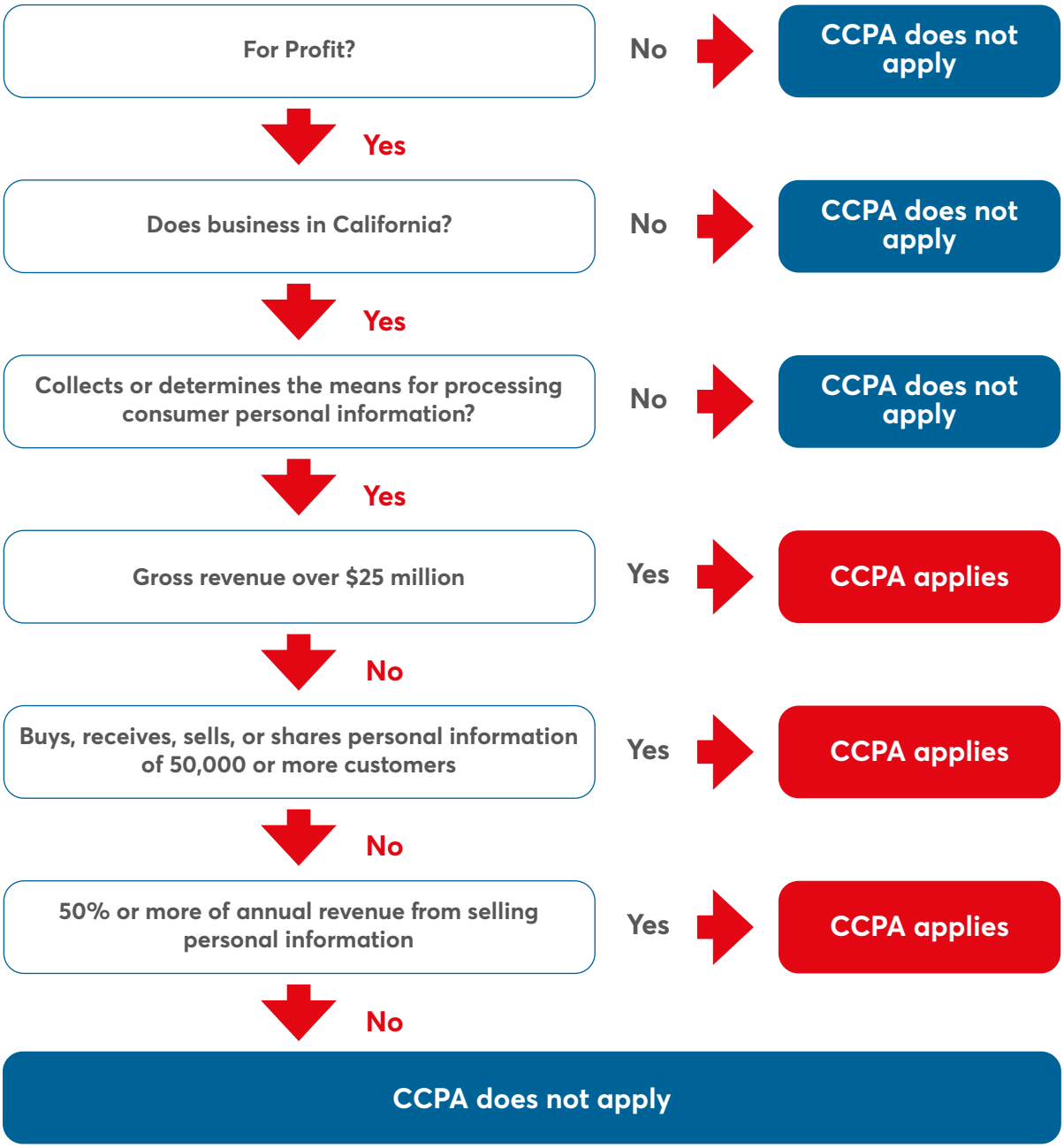
Before we investigate the unique challenges staffing agencies face when dealing with CCPA, let's take a look at who it applies to first. To qualify, you only need to meet one of these criteria:

Entities processing personal information with annual gross revenue in excess of $25 million

Those who annually buy or sell for commercial purposes, information of 50,000 or more Californians, households or devices (or organisations that derive 50% or more annual revenue from selling such information)

There is also a separate bill still under consideration in California, AB-2546, targeted at strengthening anti-spam laws and moving California (and in effect the rest of America) away from opt-out marketing permissions.

Is your organization affected?



* Certain exceptions exist and you should always confirm the legal applicability of the CCPA with trusted councel.

**A company may be considered a 'business' and subject to CCPA requirements if the company is a part or subsidiary entity that controls, or is controlled by, a 'business' and shares common branding with the business.

***If CCPA doesn't apply, other states legislation could still apply.

How a 'consumer' is defined under CCPA

Some of the biggest debate surrounding CCPA has been focussed on the use of the term 'consumer'. The term is used in a broad context and relates to any natural person who is a California resident. Where it becomes confusing is that 'consumer' also pertains to the employees of a company. Strikingly, it is irrelevant that the relationship to the natural person is as an employee and not as a consumer of a business's goods or services.

Another interesting dimension to the 'consumer' definition is how residency is defined. Residency is determined by whether an individual is:

1. in California for other than a temporary or transitory purpose
2. domiciled in California but temporarily or transitorily outside of California

To clarify, this means that employees who live in California, but might be temporarily outside of California on business, are still considered 'consumers' under the CCPA. However, employees that are based elsewhere and travel to California for business temporarily (and most importantly do not live there) are not considered 'consumers'.

The final area of confusion companies often face is whether the law applies to them if their company is not based in California. Quite simply, it does. Californians make up 1 in 8 US residents so even if the consumer isn't in California, your company still needs to adhere to best practice. There is a high likelihood you will interact with Californian residents, therefore we recommend you adhere to best practice.

What is Amendment AB25?

Due to the new interpretation of 'consumers' under CCPA, a temporary amendment has been introduced; Amendment AB25. This is significant for staffing agencies due to the types of people covered under AB25 and many of the CCPA requirements would not apply until January 1, 2021. However, it is vital not to become complacent, even with these exemptions in place, as we'll explain later.

Amendment AB25 excludes the following people for a one-year grace period before enforcement will take place:

- Job applicants
- Employees
- Contractors
- Medical staff members
- Owners
- Officers
- Directors

Another layer of complexity is added to these roles as contractors, medical staff members, owners, officers and directors would become newly defined terms provided their information is used solely in the context of their current or former role with a business. For further clarity, 'contractors' are broadly defined as a natural person who provides a service to a business with a written contract.

As an organization, it's easy to see the complex landscape companies are navigating when determining whether or not 'Consumer' data is protected or not.

It is also worth noting that Amendment AB25 excludes personal information under the following two circumstances:

01 Information that qualifies as emergency contact - If the information gathered is used solely for the purpose of having an emergency contact on file.

02 The sharing of personal information in order to administer benefits to relatives - again, if it is only for this purpose.

However, it is important not to get a false sense of security under Amendment AB25. Preparing for such monumental changes takes time, and by preparing for the amendment ahead of 2021, you're giving your organization a fighting chance to implement an effective, robust solution that will serve your needs for the long term.

For example, for these types of 'natural persons' the following CCPA provisions have come into effect on January 1, 2020:

- **the obligation to notify these individuals about the categories of personal information that the business collects and the purposes for which the information is used, at or before the point of collection;**
- **consent would still be required to collect additional categories of personal information or to use previously collected personal information for new purposes; and**
- **these individuals could still assert a claim under the CCPA's private right of action for cybersecurity incidents.**

Here, we can see that "a 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" would immediately be entitled to the rights under CCPA. With consumers more aware than ever of the power their data holds and the responsibility organizations have to uphold best practices, it's clear that companies need to stay ahead of the curve to meet the demand and expectations of consumers.

Pair this with the increasingly more likely chance for an organization to be hit with a DSAR (Data Subject Access Request) and it's clear to see staffing agencies are working in an increasingly volatile landscape. AB25 is a temporary respite and isn't something organizations should see as a get out clause.

It's important to remember that individuals can claim up to $750 if their data is misused. So whilst temporary allowances have been made, compliance is inevitable for staffing agencies and still needs to be considered a top priority, as those who don't meet compliance standards will still face fines and long term damage to their reputation.

The biggest challenges staffing agencies face with CCPA

Outside of the challenges of Amendment AB25, there are several unique hurdles that staffing agencies need to overcome to ensure they're meeting best practice standards. And with continually developing and amended bills being pushed to pass through California Assembly, it's fair to say that the hurdles will keep presenting themselves.

With that in mind, what challenges does this legislation bring about for staffing agencies?

We've identified six key areas:

- **Challenge 1:** The varying state laws and federal standards being enacted
- **Challenge 2:** Maintaining data records while remaining compliant with CCPA
- **Challenge 3:** Managing client data across multiple departments
- **Challenge 4:** Handling Data Subject Access Requests (DSAR)
- **Challenge 5:** Adapting to the ever-changing legal landscape
- **Challenge 6:** Understanding the impact of international legislation

Now; what do each of these challenges look like close up?

Challenge 1:

Varying state laws and federal standards being enacted

Over the past 12 months, privacy regulations have undergone some of the most significant changes ever seen in their history. It's a volatile landscape for compliance with complex rules and state-specific changes to law to adhere to; there is no single data protection legislation in the United States. It's a tapestry of hundreds of laws at both a state and federal level. Whilst the rules may be different per state, their goal is always the same; to protect the personal data of U.S residents.

With candidate information being shared from different states or people moving from one state to another for job relocation it is vital to be aware of the laws in each state and how it affects your staffing agency.

With governance, risk management and compliance always evolving there has never been a more demanding time for compliance officers. The need to keep pace is not only vital to business success but integral to a company's reputation. With new regulations constantly surfacing and laws in a state of flux it's essential that compliance officers can work in an agile and adaptable way, remaining confident in their approach. Their job now is not only to stay compliant but to educate other staff members and improve processes continuously.

Challenge 2:

Maintaining compliant data records

Staffing agencies rely on the volume of candidate data they hold; so the larger the data pool they have, the more candidates they can present to their perspective clients. So, the reason this is an issue is that anything that limits their data records is going to be viewed negatively by staffing agencies.

Also agencies are handling large pots of data and have entire teams dedicated to filling up their data pools with more records, yet they don't have tools in place to record what each individual candidates consent and marketing preferences are.

Challenge 3:
Managing client data across multiple departments

It is common for staffing agencies to use manual processes, across multiple platforms and tools to source and store candidate information. What's difficult is trying to pinpoint where all of someone's information is being stored, who has access to it and how up to date it is. For example, it would be a common occurrence for personal data such as someone's name, email address, phone number, photo and salary information to be stored on a centrally managed database. However, it is also likely to be stored separately by individual recruiters on their cell phones and tablets in things such as 'hot lists'. How secure is this information across all of these devices and with multiple people interacting with it?

On top of this, there's also social media to consider. Just because a candidate shares their information somewhere such as a job board or LinkedIn, it doesn't give the recruiter the right to automatically process that personal information. For permission to be granted, recruiters need to confirm with the individual (who's information is being handled) what their personal data will be used for, who will be able to view it, where it will be stored and how long the recruitment agency intends to hold onto it. Another dimension is when vulnerable people are involved in the recruitment process; all of the above needs to be explained to them in a way they understand. With a lack of clarity around how this data is being processed, it's easy to misconstrue the actions of a recruiter as trying to profit from someone else's data.

The guidance is clear; you need to be able to provide an auditable trail of how information was gathered, how you communicated your intentions to the candidate and what you intend to do with the information after interacting with them. Can you say, with confidence, that you can do this now?

Challenge 4:

The nuances within CCPA specifically regarding employees

The CCPA has been criticized for some of the grey areas it has produced, and for staffing agencies one of the most confusing is the terminology around employees as consumers.

As discussed earlier, the term 'consumer' covers employees in certain contexts, but more confusingly still the CCPA also states that information can be handled, provided their information is used solely in the context of their current or former role with a business. How do staffing agencies define what would be considered outside of someone's current or former role? Are they still marketing to these people? Are they doing it lawfully? It's a complex and potentially time-consuming task to figure out. By utilising solutions and approaches that takes this task away from you you'll be able to locate, contact and communicate with candidates with confidence.

Challenge 5:

Adapting to the ever-changing legal landscape

Once you've begun to tackle the challenges you're facing now, what about the future? Meeting the standard now, may not meet the standard in the future. With disruptive technologies such as AI being used to scrape social media platforms, carry out linguistic analysis of writing samples, the introducition of game-based assessments and ITP (Intelligent Tracking Prevention) to give consumers more control over their online privacy experience, staffing agencies are going to struggle to know if what they're doing is legal, in this new technology-driven landscape. Whilst these new technologies can help to recruit top talent and help better understand what motivates people, it also opens a host of questions around bias, accuracy, data privacy, legality and employee trust. Are you prepared for this new approach? Will you be able to adapt in an agile way?

Challenge 6:
Understanding the impact of international legislation

Does your staffing agency work with businesses and candidates at an international level? If so, the European Union's GDPR also needs to be taken into consideration when handling people's data. The table below helps to provide clarity on the differences in the international laws and how they affect California-based companies.

GDPR	CCPA
Consumers must opt-in for their data to be processed	Consumers can opt-out of their data being processed
Consent, and how it was gathered, must be clearly documented and easily auditable	Consent, and how it was gathered, must be clearly documented and easily auditable
Refers to "EU data subjects" without specifying residency or citizenship	Applies to California residents
Applies only to individuals	Applies to data linked to specific households
Applies to any business that is collecting and processing data, regardless of the business location	Applies only to businesses 'doing business in California'.
Applies to all organizations both private and public	Applies only to for-profit firms that gross above $25 million per year, deal in the personal data of 50,000 or more consumers, and derive half their revenue from selling that data

What personal data is held by staffing agencies?

With the challenges clearly laid out, it's important to gauge the types of personal information staffing agencies commonly handle. This information can broadly be referred to as Personal Information or PI.

Personal Information ("PI")

Whilst the definition given with CCPA has been criticized for being broad, "Personal Information" relates to "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Sec. 1798.140(o)(1).

Specific examples for staffing agencies include:

- New hire/onboarding paperwork, including resumes, employee applications (typically including Social Security Number, drivers' license, mailing address, and other personal information), background checks, IRS Forms W-4 (withholding), etc.
- Payroll information, including employee bank account numbers for direct deposit
- Credit card information provided in connection with expense reports
- Random drug testing paperwork and results
- Documenting of various types of leave, such as sick leave, vacation, paid time off, FMLA leave, USERRA leave, maternity/paternity leave, etc.
- Employee benefit plans (to the extent not exempt from the CCPA)
- Employee's online activity on a work computer/system, such as browsing history, search history, and information regarding the employee's interaction with an Internet Web site, application, or advertisement

Source: JD Supra (2019)
https://www.jdsupra.com/legalnews/ccpa-guide-does-personal-information-87475/

What are the dangers of not being compliant?

In today's climate, it's easy to understand why people find it difficult to trust how their personal information is stored and secured. Couple this with the extreme time pressures staffing agencies face to identify, attract and secure candidates as well as handling huge data sets (where consent can be easily lost) there are plenty of dangers to be aware of and prepare against.

By being a staffing agency that stays ahead of the curve and invests in solutions prior to the compliance deadline, your company has the chance to become a market leader. With that in mind, we've identified three of the biggest dangers of not being compliant:

The loss of your client's trust

87% of consumers say they will take their business elsewhere if they don't trust a company is handling their data (PWC, How consumers see cybersecurity and privacy risks and what to do about it, 2017). Why should it be any different for the clients who use your services? With all of the other pressures they're facing, the last thing they want to handle is a data breach issue. By knowing they're partnering with a secure, forward-thinking staffing firm they'll know that their, and their candidate's data, is in safe hands.

It's also significant to note that there is a general feeling that consumers want the government involved when it comes to personal data but feel that companies need to bear the brunt of responsibility. Nearly 9 in 10 people (87%) feel it is important or very important that the organizations they interact with use data about them ethically. (The Open Data Institute) It's clear that your company needs to face that responsibility head on. Take the lead and become a company that goes beyond a "checklist" approach.

"25% of consumers believe most companies handle their sensitive personal data responsibly. Only 15% think companies will use that data to improve their lives."

- PWC, How consumers see cybersecurity and privacy risks and what to do about it, 2017.

Damage to your company's reputation

If your consumers lose faith in your organization, then it is likely to cause damage to your reputation. When people are unhappy they share their story with others, whether that be in the viral realm of social media or amongst friends and family.

It is apparent what this potential loss of reputation could do to your firm. Key research from PWC found that consumers are willing to forgive, but their trust can only be regained if companies implement real changes in the wake of a breach.

With just 25% of people believing companies handle their data responsibly (PWC, 2017), there is a massive opportunity for staffing organizations to become leaders in compliance and position themselves as a trustworthy, customer-centric brand. Just 10% of customers feel they have control over their personal information (PWC, 2017).

Extensive Fines

Outside of reputation damage and dissatisfied customers there is the real and worrying risk of fines. CCPA has some of the harshest fines associated to it - much more severe than EU's GDPR. The CCPA gives individuals the right to bring a civil action against companies that violate the law and states that **damages will be between $100 and $750—per individual,** if there is more proof of extensive damage. The state can also bring charges against a company directly, levying a **$7,500 fine for each alleged violation that isn't addressed within 30 days.**

Turning compliance into a strategic advantage

At the root of it, CCPA is about providing greater transparency and empowering consumers to make informed decisions about their data. It's no longer about ticking a box, potentially it's a massive opportunity for staffing agencies to seize. What used to be seen as an onerous task can now be a strategic approach to winning and retaining a happy client and candidate database.

In order for your company to seize this opportunity it's clear that you need to deliver on the following areas:

- **Be able to prove how you have acquired people's information and hand it back to them, if they ask you to**
- **Have processes in place to handle DSAR requests**
- **Transparency with full audit trails**
- **Future-proof your company against regulation or industry changes**

To help meet these demands you need a robust solution and processes in place. Considering how hard it is to maintain data without a robust solution, how aware consumers are of how valuable their data is and the changing, volatile landscape staffing agencies find themselves operating in, it's clear that those who embrace technology will prosper in the long term.

Delivering on this shouldn't be seen as an unyielding and impossible task; it's quite the opposite. By putting the proper systems in place you'll be able to create an efficient, long-lasting, flexible framework. With this new framework in place, you can free up your staff's time away from menial tasks and onto a new way of working.

How to ensure you stay compliant

Utilising a Consent and Preference Management Platform enables your organization to easily meet CCPA compliance, ensuring your organization is not at risk. A Consent and Preference Management Solution enables your staffing organization to meet all five stages of the CCPA, without disruption to day-to-day business operations.

These five key areas include:

05 **Transparency –** Website operators need to offer a do not sell link to their website, among other contact methods, and that website privacy policies are updated every 12 months

05 **Access –** Individuals have the right to access any information an organization processes about them in the last 12 months

05 **Object –** CCPA is focused on preventing the sale of personal data and discriminatory repercussions for exercising rights. This means a customer cannot be denied goods, services, charged a different price, or received a reduced rate of service because they have requested their data information

05 **Deletion –** Individuals are allowed to request deletion free of charge; which must be honored within a given timeframe

05 **Portability –** Individuals have the right to move their data free of charge via an electronic, readily usable format

A Consent Management Platform allows your organisation to meet CCPA compliance by:

- **Simplifying audits and subject access requests**
- **Always being up-to-date with changing multinational laws**
- **Offering a user-friendly interface that empowers teams to efficiently respond to candidate and customer requests**
- **Ensure global compliance over multiple regional legislations**
- **Integrating easily with other systems to ensure minimal disruptions**
- **Offering granular-level consent to customers, putting them in the driving seat of their consent management**
- **Enabling you to manage multiple brands from a single user interface across**

Get in touch today

Get in touch with our team to find out more about Cassie to become compliant today.

enquiries@syrenis.com
+44 1928 622302

Meet Cassie

Syrenis has over 20 years experience in the data privacy industry and has been developing innovative solutions to tackle the challenges of an ever changing regulatory landscape. Our market-leading solution, Cassie, is utilized by organisations globally to minimise compliance risks and maximise customer data. Cassie is a fully scalable solution that integrates into your existing infrastructure causing minimal disruption to existing operations. Enabling your organisation to have one central system that works alongside your existing systems to give you a holistic overview of your customers data.

Software created by

SYRENIS

/syrenis_ltd

Vanguard House
Sci-Tech Daresbury
Daresbury
Cheshire
WA4 4AB

www.syrenis.com

/company/syrenis-ltd