



The Question PEOs and Staffing Agencies Will Be Asked Most in 2023: “Will You Delete My Data?”

Insights

1.04.23

The biggest challenge that most PEO and staffing agencies will face in 2023 will come in the form of what appears to be a fairly benign request, but one that will occur with both increasing regularity and legal significance: “Will you delete my data?” As more people are armed with information about their data privacy rights, and lawmakers and regulators continue to create additional obligations for businesses, you may field this request more than any other in the new year. And PEOs and staffing agencies face unique challenges given the amount and types of data they maintain. We’ll dive deep into this topic during the Data Privacy session at the [Fisher Phillips’ PeopleLaw Conference from February 22-24](#), but this Insight provides an overview of the topic and some initial steps to consider.

Data Deletion Overview

For those who need a crash course on what we’re talking about, we’re referring to an individual’s right to request deletion of their data from your possession. And when we refer to “data,” we mean information like names, phone numbers, email addresses, social security numbers, healthcare information, drivers’ license numbers, account numbers, financial information, photos, and a trove of additional detail.

Lawmakers and regulators have increasingly given individuals the right to have this information deleted in large part to protect consumers from harm if your systems are hacked in a data breach. Concerns also exist around your use of this information for what you consider legitimate business purposes but consumer advocates believe is a misuse of data. As a result, your business very well may be obligated to delete information upon request – or at least manage the inevitable flood of requests that will soon come your way.

Why This Isn’t Just a California Problem

You might think you only need to worry about these issues if you’re a business located in California, but you’d be wrong for three big reasons.

First, the groundbreaking California law that ushered in this new era of data privacy – [the California Consumer Protection Act \(CCPA\)](#) – is incredibly broad in its scope. It may in fact ensnare your business into an obligation to delete even if you have no physical presence in the state. You might be considered to “do business” in California, even if you merely operate a website in which California

residents provide their personal information. And one remote worker in California may also be sufficient for this law to apply.

Second, an increasing number of states are beginning to follow California's lead and implement some version of a data privacy law that includes a right to delete. Virginia, Colorado, Connecticut, and Utah have all passed consumer privacy laws that go into effect this year, and we may see New York, Massachusetts, Michigan, Ohio, Pennsylvania, North Carolina, and Minnesota follow suit soon thereafter.

Third, with this patchwork of regulations unfolding at a rapid pace, a number of larger companies have decided they will comply with the CCPA across the country in order to ensure compliance. Still other companies have chosen full voluntary compliance in an effort to demonstrate good corporate citizenship and remain competitive in the marketplace. You may want to consider a similar approach depending on your circumstances.

PEOs and Staffing Agencies Face Unique Challenges

When it comes to collecting and storing – and then deleting – data, perhaps no industry faces more unique challenges than the PEO and staffing communities. First and foremost, PEOs have in their possession information about all of their clients and their clients' employees. Second, staffing agencies have not only their employees' information, but all of the information of the temp workforce that they assign out to client worksites.

The sheer volume of data on hand dwarfs all other companies your size. This not only makes you an attractive target for cybercriminals, thus amplifying security concerns, but it also means you have to juggle more information than your resources might otherwise handle.

Moreover, you have unique challenges when it comes to all of this information. With staffing agencies, for example, you need to use data across entities and share it with clients on a regular basis. Some temporary workers move from assignment to assignment on a daily basis, meaning the number of entities and relationships you need to manage from a data privacy perspective could increase by the day.

Some Necessary Steps in 2023

It is far beyond the scope of any Insight to provide a step-by-step guide for how to manage a data deletion request, but we can provide an overview of the pathway you should follow. The key to understanding your obligations when it comes to data deletion is that **each request needs to be handled on an individualized basis** and that there may be no easy cookie-cutter solution.

First, you should acknowledge the request by communicating with the requesting individual. Next, you should determine whether you have an existing relationship with the individual making the request. If so – if they are a current employee, let's say – you may be off the hook for the time being

given that you need to maintain the information (or at least a significant portion of it) for the purposes of running your business and managing the employment relationship. The CCPA provides eight specific exemptions that permit you to reject a deletion request, and one of those involves the current employment status of a requester.

If they are a former employee, you might still need to retain all or a part of the information you have in your possession. There may be legitimate business or legal reasons (such as record retention laws or other legal compliance or defense needs) for you to hold on to some or all of the data.

Whatever you end up doing with the data – deleting it all, retaining it all, or deleting just a portion of it – you need to make sure you properly process the request, respond to the data deletion request, and document the entire chain of events.

Is 2023 The Year You Automate?

If your organization receives 10 or more consumer requests per month, you've hit the magic number that might make you want to automate your processes. After all, some responsibilities under the CCPA require you to act within 45 calendar days, while others involve a short 15-business day turnaround. If you can't handle the volume of requests sufficiently, you run the risk of violating the law – and California's law carries some significant bite. Civil penalties start at \$2,500 per violation (and could rise to \$7,500 for intentional violations), and data breaches involving certain sensitive personal information can give rise to individual or class action lawsuits.

The law includes a "private right of action" allowing California residents who prove that a data breach resulted from a failure to implement appropriate security measures to recover statutory damages between \$100 and \$750 *per person, per incident*, even if they cannot prove actual harm, or their actual damages if provable, whichever is higher. These penalties can add up quickly, particularly in a class action context. For these reasons, it's best to have a robust deletion process in place to ensure you have eliminated information you'd rather not have on hand if a breach occurs.

If your business is overwhelmed with manual responses, automation may be your ticket to safety. But you'll want to work with your Fisher Phillips Data Privacy attorney to vet the many possible software providers that provide the necessary services and select the right one. Your attorney can help you choose the providers to interview, run demos with them, ask the right questions, and generally facilitate a fruitful discussion to steer you in the right direction.

PEOs and staffing agencies have specific business needs that often require a deeper investigation than a typical company when it comes to selecting the right provider. We find that the best providers are the ones that connect with your preexisting applications and technology tools you already have in place to manage your data, and also take into account your existing business approach. Partnering with a trusted team of PEO and staffing lawyers with experience in the data privacy world will make all the difference.

Learn More

We invite you to join us in Marina del Rey, California, for Fisher Phillips' first annual [PeopleLaw Conference](#) on February 22-24, where we'll discuss this – any many other topics – in depth. We'll bring together thought leaders in the PEO, staffing, and gig economy industries to discuss common legal challenges and solutions, and you'll hear from our firm's PEO and Staffing Group lawyers, along with industry association executives, on the latest trends in a series of engaging and interactive sessions. Each session will provide you practical skills you can put to use right away. You'll also have plenty of time to network with your peers to gain invaluable insights and learn from each other. [You can learn more about the conference and register by clicking through here.](#)

Until then, we will continue to monitor the situation and provide updates as more information becomes available. Make sure you are subscribed to [Fisher Phillips' Insight system](#) to get the most up-to-date information. Any questions may be directed to your Fisher Phillips attorney, the authors of this Insight, or any attorney on our [PEO and Staffing Industry Team](#).

Related People

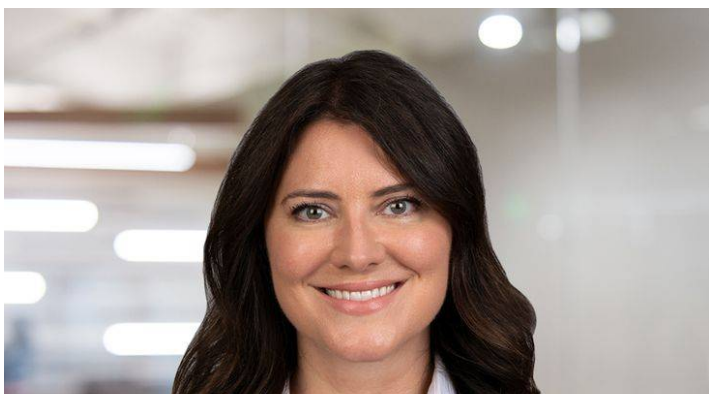


Usama Kaht, CIPP/US

Partner

949.798.2118

Email





Anne Yarovoy Khan

Of Counsel

949.798.2162

Email

Service Focus

Privacy and Cyber

Industry Focus

PEO Advocacy and Protection