exterro

DATA PROTECTION WORLD FORUM

The 3 Biggest Mistakes Companies are Making with CCPA

The 3 biggest mistakes companies are making with CCPA

With the California Consumer Privacy Act (CCPA) officially launching January 1, 2020, many organizations are still playing catch-up in determining exactly how they'll comply with major provisions before full enforcement begins July 1, 2020.

So far, the biggest risks stemming from the CCPA have touched on a few major areas: the ability to respond to consumer requests for data, breaches of personal data and the resulting fines, and maintaining proper preservation of data needed for civil or criminal litigation. Below, we'll take a look at each of these commonly made mistakes that companies are making, and offer a roadmap to CCPA compliance.

Most of the mistakes that businesses and individuals are currently making regarding their compliance efforts fall into one of the following three categories:

- Failure to harmonize the DSAR process with litigation requirements
- Forgetting to include paper records in the DSAR process
- Over-retaining data, which heightens the potential impact of data breaches

In this guide, we'll look into each of those obstacles and offer defensible practices to avoid adverse legal and financial consequences.

Exterro whitepaper contents:

#1

Data Subject Access Requests (DSARs) are a key feature of both the CCPA and the EU's General Data Protection Regulation (GDPR). They allow an individual to request to know what data a business holds on them, and ask that it be deleted. Under the CCPA, a business has 45 days to fulfill a DSAR.

DSARs are fraught with risk: The timeline is tight for any organization that doesn't have automated processes and workflows to answer these requests, they're expensive to respond to (Gartner reports that it costs about $1,400 per request) unless technology is used, without a data inventory it can be difficult to verify that all of the information has been turned over or deleted.

But what if that data requested is already legally-bound by another law or regulation, and therefore required to be saved under a legal hold?

Deleting data that is this potentially relevant to anticipated or pending litigation (civil or criminal) can have devastating consequences, making it imperative that any DSAR process must harmonize with information under a legal hold. How do you go about squaring a customer exercising their right to have data deleted with the legal requirements that that same information be saved?

Considering the speed at which many companies are trying to, in many cases, delete data (45 days, as required by the CCPA, or 30 days, as required by the GDPR), it's not hard to see how mistakes can happen if processes aren't connected and people aren't communicating.

The recommendation:

There are four primary considerations with DSARs:

Time

How long does it take to fulfill a single request?

Cost

How expensive is it to fulfill a single request?

Scale

Is your process able to maintain efficiency even with a 10-fold or 100-fold increase in the number of requests?

Risk

How do you know you're handing over all of the correct information to the correct individual in a secure manner — and not deleting legally-protected material?

The request answering process that your organization builds should consider where it makes sense to cross- reference the DSAR request with the person or team in charge of legal holds, and verify that the information can be deleted.

MISTAKE #2

Not including paper in your DSAR process

#2

Paper records have become close to an afterthought in our digital world, but many companies that have been around for decades are still likely to have filing cabinets or boxes filled with documents that they really don't need.

But those records still count as data, and still must be produced during a consumer request. So even if it seems that paper records are harmless, they're largely the subject of GDPR requests involving employees of former businesses: They want paper documents.

The CCPA doesn't delineate between electronic and paper data. Plaintiff's attorneys seeking large settlements due, for example, to a termination in which an employee is seeking all of the information held on them want to make it difficult on that business to produce everything. Therefore, paper is a bigger threat to compliance than it may seem.

In fact, the first fine issued under the GDPR had to do with over retention of paper data. Doorstep Dispensaree, a London-based pharmacy, housed boxes of paper documents of patient records in an unsecured shed on the business's property. The documents were back- dated further than the retention laws of the GDPR allows, therefore leading to the violation.

The recommendation:

Organizations should try and work towards making all data digital, and removing the need for storage of paper records entirely, if allowed by the regulations that govern your industry. This means reviewing paper records and transferring that data to a digital means which, ideally, would be easier to keep track of and inventory.

If paper records must stay a part of the business, then it's even more important to follow data retention laws, for which most major data privacy laws have a provision. In fact, the Irish Data Privacy Order addresses this in a handy checklist on their site, offering a couple of questions to clarity data retention and minimization requirements:

- Is the personal data limited to what is necessary for the purposes for which it is processed?
- Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected?

Whether it's paper or digital, the question remains the same: Why are you retaining the data in the first place? Does it have a business purpose? There's a good chance many of those paper records serve no business process, so review and disposal in the name of better compliance should be a priority.

#3

In recent years, high-profile data breach cases ranging from Equifax to the recent Hannah Andersson data breach—the first class-action lawsuit citing the CCPA—have forced larger companies to put cybersecurity on their radar of business needs. With Marriott and British Airways both facing record fines due to data breach violations under the GDPR, major companies are officially on notice that cybersecurity is no longer optional.

While full enforcement of the CCPA won't start until July 1, the data breach provisions—along with resulting fines and class-action suits that an organization might face for a breach—actually began on January 1. Only a month later, a high-profile class-action suit was filed.

Over-retention of data also has negative impacts on litigation. The more data that is just sitting in organizational repositories, the more there is to sift through if a discovery request is made. This means that there are larger volumes of data to collect, sift through, and review: An expensive and time-consuming conquest. Unfortunately, it also means that there is likely to be more relevant information to uncover and produce—which could end up being a negative during the course of the litigation.

If there is one, crux issue that affects most other downstream processes and is most likely to lead to fines, it would be over-retention of data.

The recommendation:

Businesses need a plan to reduce their volumes of data for reasons pertaining to litigation and data breach risk.

There are two good reasons to create and enforce retention policies at any business:

01

Data you don't have can't be breached. You don't have to protect data that you don't have. And, with respect to DSARs, you don't have to spend time and money searching for data you don't have.

02

To minimize the impact of e-discovery on litigation, either current or in the future.

We're still early in this new era of data privacy regulations, and already the astronomical fines are grabbing headlines. Building and enforcing retention policies that are in line with major compliance rules can help prevent enterprises everywhere from becoming the next big headline and reducing potential monetary liability that may occur if your data is ever breached.

exterro

FUTURE-PROOF YOUR COMPLIANCE APPROACH

Get ahead of the coming regulatory onslaught by preparing your organization now with automated processes and technology that facilitates easy compliance with the CCPA, GDPR, and other data privacy regulations. Request a demo of Exterro's Legal Software Suite, the industry's only Legal Governance, Risk, and Compliance (GRC) platform, and see how future-proofing your compliance approach can pay dividends in cost avoidance.

GET A DEMO

Contact details

info@exterro.com

Headquarters: 503-501-5100
European Office: +44 (0) 203 858 9587
St. Louis Office: 636-778-1700



Visit Exterro

exterro®