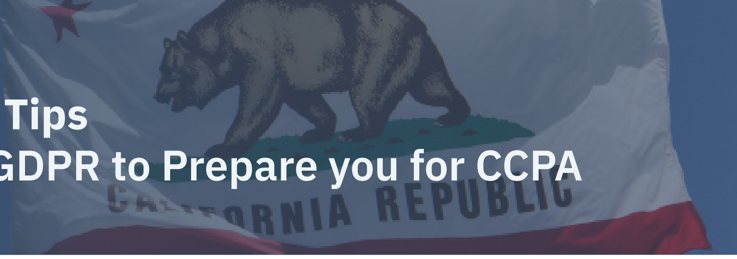
CENTRL



Top 5 Survival Tips Learned from GDPR to Prepare you for CCPA

Rising consumer expectations and empowered mindsets are creating a new landscape of risk for privacy professionals.

The time to comply with CCPA mandates is right around the corner. Some organizations are taking a “wait and see” approach, thinking there is still plenty of time to get started. After all, CCPA fines and penalties aren’t enforceable until the summer of 2020. But most agree that CCPA is here to stay and any anticipated amendments aren’t going to take any teeth away.

Then there are the holdouts who think they can wait until the Federal Government enacts overall privacy legislation. But the fact is, every state already has their own data breach notification and disposal laws. Without a Federal mandate to look to, twenty-five states are already in the planning stages of developing their own privacy laws. And CCPA has paved the way for at least 15 similar regulations in Maryland, Nevada, Massachusetts, Rhode Island and other states.[1]

Different philosophies about what is considered personal data can also get in the way of enacting your CCPA program. Some think depersonalization and pseudonymized of consumer data will protect them from having to comply. However, CCPA amendments still keep some definitions intentionally vague, stating that consumer data cannot be considered depersonalized if it can be “reasonably” linked to a consumer household. And while there are no specific security activities that are prescribed, your privacy and security practices better hold up to what the California Attorney General considers to be “reasonable.”

GDPR is just a little more than a year old. Organizations that needed to comply with GDPR and took a wait and see approach to GDPR compliance, got a firsthand look at the ruckus created when these mandates go into effect.

Let’s examine the top ways GDPR has impacted organizations and how you can strengthen your privacy program to survive the rigors of CCPA.

> *“Whereas many organizations may be focusing on the fines or the litigation, subject rights requests left unmanaged have the potential of becoming ‘death by a thousand cuts’ and costing the organization millions of dollars on an ongoing basis.”*
>
> How to Prepare for the CCPA and Navigate Consumer Privacy Rights, Gartner Report, June 12, 2019

Impact #1 Manual Subject Access Request Tasks Drains Privacy Staff Productivity

Enormous fines and data breach notification requirements get all the fear, uncertainty and doubt when it comes to GDPR and the upcoming CCPA mandates. Yet the failure to respond to data subject access requests has been called "death by a thousand cuts" by Gartner.

It is estimated that by 2021, less than two years away, 80% of the negative financial impact of CCPA will come from failure to implement a scalable subject rights workflow. [2]

When considering the impact of CCPA on your organization it is important to put these numbers in perspective with the fact that GDPR has served to greatly educate consumers. And DSARs are what is increasingly being used by these individuals who are exercising their rights. [3]

For example, Microsoft waded through 18 million requests people submitted during the first year of launching their global privacy self-service portal. Finally, it's hard to get the full picture of the impact of responding to DSARs without mentioning how long respondents indicated it takes to respond to a DSAR. The majority of organizations receiving DSARs are taking a full working week to respond to each, at an average cost of over $1,400. [4]

Survival Tip #1

Manual tasks, Excel spreadsheets and ad-hoc processes are what keeps your staff constantly treading water. Any unusual influx of DSARs, and they won't be able to keep up under the extra burden. Consider a solution that can automate tedious tasks and integrate with your existing workflows.

Look for a solution that can streamline key privacy program workflows, including:

Issue Tracking Workflows
When a Data Subject Access Request is received, it should directly flow into the issue tracking systems you already use. Like Jira or ServiceNow or others that you use to track and resolve programs. There is no need to create another workflow.

Intake Processing
If you already use an opt-out form, there is no reason to create a new one. Consider solutions that work with the forms and tools you already use so there is no need to force your staff to learn new workflows.

Communication
Use the tools that work best for your organization. You don't need a separate communication system; use the communication avenues that everyone is already using.

Identification and Verification
There's no reason to create new logins to verify the identity of subject access requests. You can use a simple email address or leverage existing tools that already verify identity. Look for solutions that have integration capabilities that go beyond simple SSO and AD.

Impact #2 Breadth, Volume and Depth of Data Required to Fulfill a DSAR is Overwhelming & Prone to Human Error

Who knew a simple DSAR request could unearth so much data? As a privacy professional, you probably don't relish the idea of having to extract subject access data out of back-office systems. It's not just data, emails, and html files that you need when completing a subject rights request. There is a complete range of consumer data to be mined with each request.

This is especially true if you work for a company with multiple customer communication channels or use IoT devices to store customer data, for example video doorbells and smart appliances. In these cases, fulfilling a DSAR request is no simple look-up procedure. Most times, the data will look just as unfamiliar to you as it will to the individual requesting it.

To demonstrate the breadth of data required to fulfill a DSAR, consider the case of Jon Porty, a reporter at **The Verge**. He decided to take a test drive of the subject access request process at the biggest tech companies in the EU: Apple, Amazon, Facebook, and Google. Jon started his journey by going through a dizzying array of consent portals and forms to get his data.

Thirty days later, he received a motley looking package of what was presumably his data. There were old phone calls, SMS messages, web and location tracking info. For example, Google provided Jon with a 61MB JSON file with all of his location history. In the end, he received 138GB from the four company's he contacted.[5] But his data might as well have been an ancient form of hieroglyphics for how much sense it made.

Then there is the human-error side of things that can lead to less than optimal results. Let's take a look at what happened to Martin, a German consumer who put in a seemingly innocent subject access request to Amazon in 2018. To protect his identity, Martin is not his real name. The information he got back from Amazon was a gigantic data file that he was truly not expecting.[6]

To his surprise, Martin received thousands of Alexa recordings from Amazon. But Martin has never owned an Alexa-enabled device, so this was quite a shock. After trying to contact Amazon to no avail he got some reporters from the German magazine **c't** involved.

What makes this story noteworthy is that the recordings were so numerous and detailed that the reporters were able to pull together enough recordings to identify who the recordings actually belonged to! And of course, afterwards the reporters from **c't** interviewed both Martin and the person that the recordings belonged to and published a rather scathing article on Amazon's privacy practice.[7]

Survival Tip #2

Mining for data subject files in response to a DSAR means you have to look through all your own internal repositories, email, voice recordings, and all the other ways you track consumers.

Extend your search beyond your own systems to 3rd parties. These could be companies you use for customer communications, outreach, marketing analysis, support services, regional events and so on.

Deep integration within your own systems and third-party SaaS and services is the only way to extract a multitude of files in a streamlined manner.

Impact #3 All Eyes will be on your Privacy Program – Most of the Attention will be Unwanted & Confusing

When January 1, 2020 rolls around expect some unwanted attention from the curious, disgruntled, privacy trolls, opportunists and just about anyone who is unhappy with your organization. Attention is going to come from some pretty interesting places.

GDPR and recent scandals at Facebook and Google has shed so much light on the way in which personal data is handled, that consumers are feeling paranoid. But they also feel empowered to request, access and delete data they never had access to before. This combination of awareness, empowerment and a touch of paranoia can have unpredictable outcomes for any privacy team.

A survey of 3,000 respondents conducted by Veritas right before GDPR went into effect demonstrates this line consumer empowerment. Forty percent of the respondents said they plan to exercise their rights within the first six months. Of the 40%, roughly 8% or 144 people admitted to just wanting to annoy certain brands out of spite or revenge.[8]

CCPA can easily be exploited by activists looking to punish a company. Career plaintiffs could use CCPA to find companies that aren't responding to DSAR requests properly. Privacy trolls are everywhere trying to look for failures by out-of-state companies that don't think they need to comply with CCPA. A quick look on reddit gives you a glimpse into the mind-set of consumers that are taking their privacy seriously and requesting their information from every organization they can think of.

You would think the curiosity-driven consumers would be less harmful, but curiosity can produce some rather odd behavior that can wreak havoc on your privacy operations.

For example, Akiva Miller who works for a data analytics company in New York recalled a recent incident where an individual visited and interacted with their website, and less than an hour later, submitted a brand new DSAR. On the surface, it doesn't seem that bad, but as Miller explained, when a DSAR comes through, her staff then has to contact multiple stakeholders across the company to determine which databases hold the data on that individual.[9]

Even Bots will take Aim at your Privacy Program

Some privacy professionals have been receiving canned bot-like messages requesting complete deletion of a user without much information to verify who it is and what exactly needs to be deleted.

That's what happened to Pegah Parsi, the privacy officer for UC San Diego. She started researching where these canned requests with little information were coming from. That's when she discovered www.deseat.me, a service that crawls through a users email to discover where a user may have signed up for something. It will then send an automatic DSAR with whatever information it is able to glean from the email. Besides the ability to send out massive numbers of requests that would overwhelm any privacy operation; the notices are intentionally vague. So, privacy organizations must perform many extra steps to find the consumers data.[9]

Survival Tip #3

Portals and login backed forms only solve part of the problem when it comes to streamlining customer requests. You need to have both request validation and identify verification.

Request Validation
Gives organization the confidence they need that a real human is making the request. The combination of CAPTCHA, email verification and threat scoring ensures the request is not coming from a bad IP address.

Identify Verification
Enables privacy organizations to only focus on verified individuals. Under CCPA and GDPR, organizations only have to act on requests once an individual has been verified to be who they say they are.

Impact #4 Third Party DSAR Requests Complicates Identify Verification

Both GDPR and CCPA allow an authorized individual to request privacy information on behalf of another consumer. There is little guidance on what this verification should look like and what are the steps to "reasonably verify" that a person is who they say they are or are otherwise authorized to act on before of the consumer.

James Pavur's story illustrates just how confused some organizations are when it comes to 3rd party requests and how to verify identify. Pavur, a PhD student at Oxford University and his fiancée were sitting in an airport lounge due to a delayed flight. They thought, wouldn't it be fun to get a little revenge on the airline that delayed their trip? Maybe spam them with a GDPR request, waste a little of their time?

It was just airport banter and they didn't follow through that day. But later the experience sparked the idea of probing the GDPR system to see what they could learn. How were all these companies dealing with these subject access requests?

His research involved testing provisions that enable authorized 3rd parties to make a subject access request on behalf of a consumer. Over the course of two months, Pavur sent 150 GDPR requests in his fiancée's name, asking for all available data on her. In total, 108 organizations replied, with 83 of the companies stating that they had information on his fiancée.

- Five companies declined any liability to GDPR rules. They were mostly US based companies that did not think GDPR applied to them
- Twenty-six companies out of the 108 just handed everything over with a simple email request and phone number
- Seventeen companies asked for additional identification

Thanks to these requests, Pavur was able to get his fiancée's Social Security Number, date of birth, mother's maiden name, passwords, previous home addresses, travel and hotel logs, high school grades, partial credit card numbers, and whether she had ever been a user of online dating services.

Even more disturbing was to see what some companies did once they received the request. An advertising company posted the DSAR request letter on the Internet. This constituted a data breach in and of itself. An organization Pavus's fiancée had never heard of, and never interacted with, had some of the most sensitive data about her. [10]

Survival Tip #4

Getting DSARs Right
The ability to socially engineer a DSAR request to get enough information to steal an identity is what keeps privacy professionals awake at night. Most often, it was the mid-size businesses that knew about GDPR but didn't have established processes and policies that failed Pavur 's experiment. The requirements and allowances provided by GDPR and CCPA is a double-edged sword that leaves privacy professionals feeling like they are going to get it wrong no matter what they do.

Identify Verification
One of the best ways to ward off these risks is to verify an identity without collecting more information. Challenge users to verify a known email address or phone number. If that's not enough, you can turn to knowledge-based authentication questions, like details about their last purchase or when they first opened an account.

Impact #5 – Longer Sales Cycles, Missed Numbers & More Assessments

One the biggest impacts that companies are experiencing with the shift to being more privacy minded, is delayed sales cycles. The fact is, privacy concerns are delaying sales cycles by a large margin. Since last year when Cisco conducted their Data Privacy Benchmark Study, just 66% of companies experienced delays. Today, that number is 87%, an increase of almost 20%.

Cisco surveyed more than 1,800 individuals with direct responsibility for privacy related concerns. Top reasons for sales delays relating to privacy include:

- Investigating specific/unusual requirements for the customer/prospect to establish their comfort with privacy practices – 49%
- Need to learn more about our privacy policies or processes – 39%
- Redesign product/service to meet privacy requirements – 38%

Over 94% of organizations reported delays up to 10 weeks with the average delay being 4.7 weeks. Shockingly, there were a few organizations that reported delays of 25 to 50 weeks or more. In summary, the least prepared organizations have average delays that are nearly 60% longer than those that are most prepared. [11]

Survival Tip #5

Act Now

Waiting around, wishing CCPA would drastically change or that somehow your company will somehow not fall under its preview, is not a feasible strategy. Don't be shortsighted and think the "wait and see" approach will somehow save you time or money later. Without enacting your privacy program now, it is more likely that you will find yourself spending considerable time waiting around for purchase orders or possibly even losing deals later. Both GDPR and CCPA make it risky to engage with vendors that do not have robust security controls and privacy practices that can be formally evaluated.

Final Thoughts and Survival Tips for CCPA

Things have changed since GDPR went into effect. As a result, consumers have more empowered mind-sets. You still have all the same customers you once knew, but they are awakening to a new normal when it comes to their privacy rights and relationship to your company.

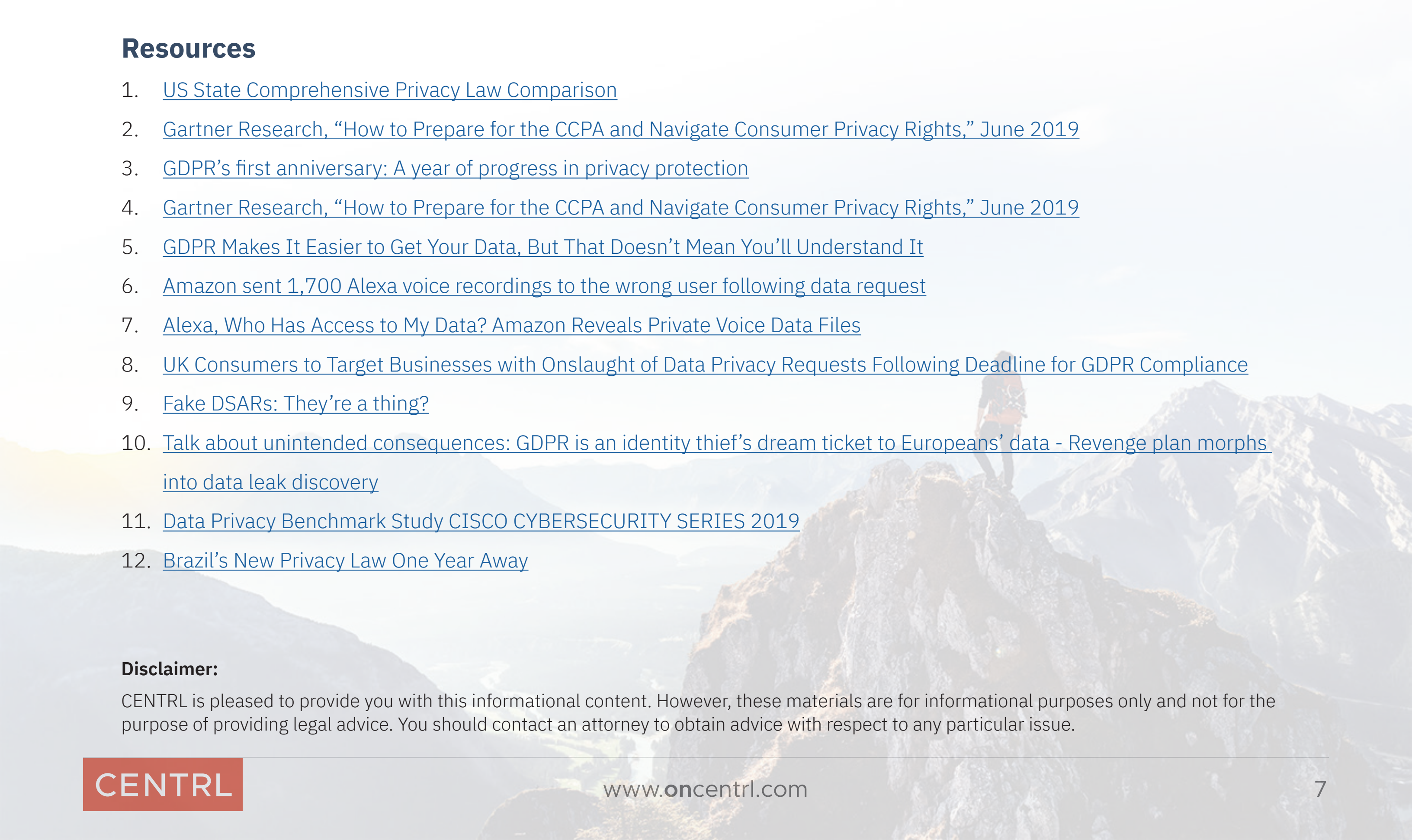
Consumers are more aware, empowered and curious about the information kept on them, how it's used, and who else has access to it. This should concern any privacy professional enough to abandon any "wait and see" approach to privacy compliance.

Along with the empowered consumer, companies who invest in their privacy programs will more closely scrutinize your organizational practices as well. Both GDPR and CCPA highlights the relationship between third parties and their data privacy measures.

Not only will your organization need to respond to increasing volumes of data subject access requests, but you can expect to respond to increased numbers of security assessments from your partners. If you are not engaging in the same activities with your own set of partners, a third-party breach is living right next door to you.

The best advice we can offer you is not to ignore what is happening around you in regard to privacy and rising tide of consumer expectations. In 2021, California organizations will need to also respond to employee DSARs. There is no slowdown or roll-back of privacy regulations that is going to happen. Right now, all eyes are on California and it's CCPA legislation. Tomorrow it will be another US state or country. [12]

Take steps now to get your privacy program under control. Save yourself from the nightmare of managing piecemealed solutions or manually fulfilling DSARs. Look for a solution that can help you engrain privacy practices into your everyday workflows, systems and the tools that you already use.



Resources

1. US State Comprehensive Privacy Law Comparison
2. Gartner Research, "How to Prepare for the CCPA and Navigate Consumer Privacy Rights," June 2019
3. GDPR's first anniversary: A year of progress in privacy protection
4. Gartner Research, "How to Prepare for the CCPA and Navigate Consumer Privacy Rights," June 2019
5. GDPR Makes It Easier to Get Your Data, But That Doesn't Mean You'll Understand It
6. Amazon sent 1,700 Alexa voice recordings to the wrong user following data request
7. Alexa, Who Has Access to My Data? Amazon Reveals Private Voice Data Files
8. UK Consumers to Target Businesses with Onslaught of Data Privacy Requests Following Deadline for GDPR Compliance
9. Fake DSARs: They're a thing?
10. Talk about unintended consequences: GDPR is an identity thief's dream ticket to Europeans' data - Revenge plan morphs into data leak discovery
11. Data Privacy Benchmark Study CISCO CYBERSECURITY SERIES 2019
12. Brazil's New Privacy Law One Year Away

Disclaimer:

CENTRL is pleased to provide you with this informational content. However, these materials are for informational purposes only and not for the purpose of providing legal advice. You should contact an attorney to obtain advice with respect to any particular issue.