HOW TO BUILD A DATA INVENTORY AT YOUR ORGANIZATION

USING TECHNOLOGY TO OVERCOME DATA PRIVACY CHALLENGES

exterro®

Solutions for Finding Corporate Data Fast

For most businesses, governments, and organizations, data is everywhere. Until recent laws and regulations establishing stringent new requirements for consumer data privacy, what happens with an individual's data after it's fulfilled its purpose could have been anyone's guess. *Analysis on Big Data* shows that the size of the digital universe doubles every two years, and that human- and machine-generated data is experiencing a growth rate **10 times** that of traditional business data. Now, governments are requiring that businesses manage and secure that data.

All of this happened—and is continuing to happen—faster than most organizations can prepare for it. As the amount of data companies and governments hold onto continues to scale upward, organizing and managing that data in a secure, compliant, and thoughtful way becomes even more important.

Exterro has put together this guide to help individuals who play a key role in managing their organization's data. With the right mix of people, processes, and technology, implementing and automating routine maintenance of your organization's data can become an efficient way to comply with new privacy laws.

Table Of Contents

1. Why It's Important to Have a Data Inventory . . . . . pg. 3

2. How to Develop a Data Inventory at Your Organization . . . . . pg. 5

3. Harmonizing Data Retention Obligations with Your Data Inventory . . . . . pg. 7

4. Managing Third-Party Vendor Data . . . . . pg. 8

5. Key Challenges of Creating and Maintaining Your Data Inventory . . . . . pg. 9

6. A Data Inventory Case Study . . . . . pg. 13

CHAPTER ONE:

Why it's Important to Have a Data Inventory

Data lives across all areas of all different departments: legal, IT, marketing, services, sales—everywhere. Often, data lives in places many of us aren't even aware of, due to either tribal knowledge that has long since left the organization or a lack of documentation and maintenance of important data sources. This emphasizes the importance of engaging leaders across the organization to help understand what is being and has been collected, with whom that data was shared, and where it currently resides.

Such an undertaking often requires a special project manager, or team (a committee of managers, for example) to help enforce data hygiene rules among departments. This team or individual would engage with key stakeholders across the business to better understand their practices around data and create a streamlined process for handling that data. The most effective and efficient way to handle your data inventory would be to use a software platform that can handle end-to-end collection and analysis of that data.

"If your data is all over the organization, it's going to be much harder to delete it, find it, access it, and centralizing its location is very important. Understanding how the data subject requests are going to come into the organization and developing a procedure for actually complying is very important. The more you can automate this process, the better. And I think at the end of the day, if companies are trying to do this manually, there are going to be trip ups. There are going to be lawsuits as a result of those trip ups, as well as regulatory actions."

DAVE NAVETTA,
Partner, Vice Chair of Cyber/Data/Privacy
Cooley LLP

CHAPTER TWO:

How to Develop a Data Inventory at Your Organization

Since all of the questions surrounding compliance to data privacy regulations start with the organization's data map, it needs to be built the right way. This means organizations should use their tools and technology to stay flexible as these laws evolve, thus keeping the data inventory modern and actionable.

There are several questions to consider when it comes to managing a data inventory, as well as relevant personally identifiable information (PII) at your organization. Take a moment to consider each of these questions to be "must know" pieces of information that your organization's data privacy officers should have positive, "yes" answers to:

- Is it easy to filter and identify data based on any parameter, including regulatory statutes?
- Is it easy to update, maintain, and ensure that the data is accurate?
- Is the data able to be identified by record type, regulatory standard, and other variables?
- Does it contain all your organization's data?
- Can it include third parties that collect and store data on your behalf?
- Can you identify the data subjects by how they interact with your business?
- Can you identify where in your business process that data is stored?
- Can you identify the business purpose for collecting an individual's personal information?
- Can you identify the collection methods of that personal information?

"Yes" answers to these questions probably indicate that a formal, structured process to keep data up to date is in place. A system of processes between departments that act as prompts to update the data inventory is also a great way to automate maintenance actions by stakeholders. And typically, the most effective way to run that automated process and maintain an up-to-date inventory of your ESI is to use a software platform that acts as a secure repository for that information.

"If you don't know where your data is and you don't know where it's being sent to, you can't comply with [the CCPA]. That's a hard stop, period."

Dave Navetta,
Partner, Vice Chair of Cyber/Data/Privacy
Cooley LLP

Technology's Role in Creating a Data Inventory

Data mapping or inventory platforms can help automate many of the key efforts involved in maintaining your data by providing repeatable processes between teams. Some platforms allow you to profile your data to identify where it's being managed, and retain it based on how it was collected—automatically connecting that data to the applicable privacy and security regulatory requirements. *High-end platforms* also provide interactive, configurable visualizations, allowing you to see the data in different ways.

CHAPTER THREE:

Harmonizing Data Retention Obligations with Your Data Inventory

Much of the data held doesn't have much of a business use. It's what's known as ROT: redundant, obsolete, or trivial data. Getting rid of this excess data is an approach often referred to as "data minimization." Data minimization is important because data you don't have can't be breached, so less data likely represents less risk. The same is true for litigation in helping to minimize the impact of e-discovery.

At the same time, there are other legal obligations, like a legal hold, that may create roadblocks in organizational attempts to delete data. Deleting data that is under a legal hold means running afoul of a different and sometimes competing regulation. That's why it is of paramount importance to do two things:

- Square data retention obligations like those created by the GDPR with those created by a legal hold or other relevant regulation; and
- Remove any and all data that doesn't serve a business purpose and isn't under a legal or regulatory hold

Regarding GDPR compliance, each category of personal data must also have a related retention period—30 days, six months, whatever the case may be. But as a general rule, the data should not be stored any longer than the business purpose for which it was collected dictates.

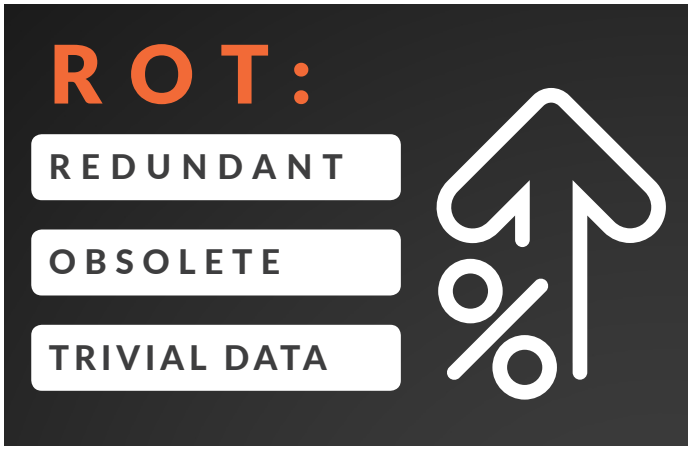
London-based pharmacy Doorstep Dispensaree actually faced a GDPR fine for this violation in December 2019: Among their regulatory violations was an over-retention of personal data. As for U.S. violations, one of the claims in the CCPA's first class-action lawsuit against Hanna Andersson in February 2020 called out negligence in deleting personal data.

The impact stretches into the e-discovery process as well. Review is by far the most expensive stage in the e-discovery process, taking up about 73% of total e-discovery costs. Holding too much data can be doubly expensive for organizations that prefer to outsource their document review, because outside counsel is essentially being paid to review extra ESI that shouldn't have been stored in the first place.

The importance of adhering to strict data retention standards can be broken down into two questions:

1. Could a demand for all documents pertaining to a specific person expose your organization's over-retention of personal data?
2. Can your organization delete excess data that would help minimize exposure to judicial and regulatory sanctions, as well as civil liability?

Put simply, data you don't store can't be breached, and you don't have to produce it during litigation. Keep only what's necessary in your data inventory—but be sure to do so while harmonizing your requirements with any relevant regulations you comply with.



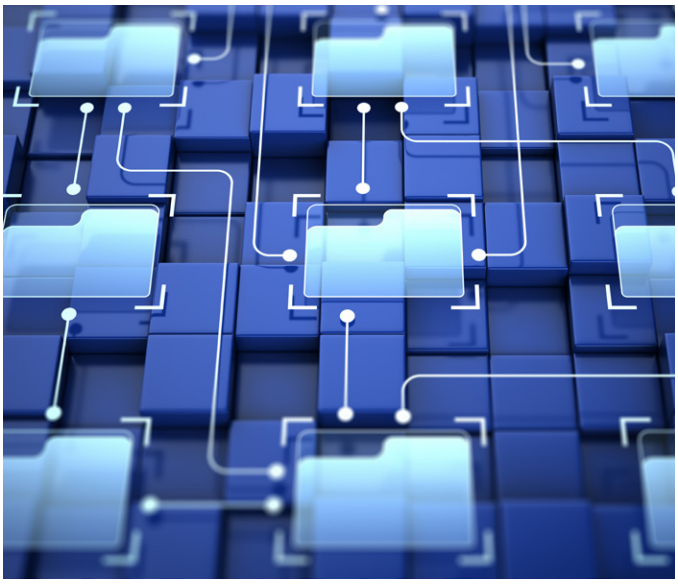
CHAPTER FOUR:

Managing Third-Party Vendor Data

Many businesses work with vendors, agencies, or other third parties that own PII. In fact, the amount of data held by third parties is usually more than most organizations think, and they happen to be the bigger target when it comes to data breaches: A 2018 study by the Ponemon Institute found that about **60%** of data breaches are caused by third parties.

Part of your data inventory should include an understanding of who those third parties are, and what organizational data of yours they have access to. This especially comes into play when considering Data Subject Access Requests (DSARs)—organizations must know which third parties have access to personal information that an individual is requesting. With new privacy regulations, businesses will have to roll new considerations into their third-party vendor management:

1. **Vendor Inventory:** Do you have a comprehensive inventory of all your third-party vendors and service providers that access, process, or store personal information on behalf of your company?
2. **Vendor PII:** Have you identified the specific types of personal information each vendor accesses, processes, or stores—and the related business processes and purpose?
3. **Process Accountability:** Does your organization have a formal, recurring assessment process in place to evaluate the data privacy and security practices for all third-parties that access, process, or store personal information on behalf of your company?
4. **DSAR Response:** Have you evaluated each vendor's ability to respond to DSARs and deletion requests?
5. **Vendor Agreements:** Have you reviewed and updated your vendor agreements to ensure they strictly limit the use and disclosure of the personal information you share with them?



CHAPTER FIVE:

Key Challenges of Creating and Maintaining Your Data Inventory

Data mapping is complex and challenging—and there are pitfalls to avoid. It's a big focus in terms of time and resources, so doing it efficiently is key. Here are four common challenges and shortcomings associated with data mapping and how they can be mitigated.

#1 The "Time-Suck"

There are ways to significantly ease the data mapping burden. It starts by defining a process for gathering information.

- In most cases, systematic interviews with data stewards are the most efficient way to collect info for a data map. These interviews should be simple and template based so that responses can be quickly interpreted and immediately incorporated into the overall plan.
- Leverage systems that can automate the interviews so that follow ups, reminders and update questionnaires can be pre-scheduled and responses automatically logged.
- It also helps to start with what you know and build out. IT teams are responsible for managing a company's data environment for operational purposes, so they will have a lot of useful information that can be used as a starting point.

"[Creating a data inventory] can become not only are you looking to see what data you have to protect it and to be compliant, but also: how can you leverage this to help your business? And that's definitely a key point [to] make to executives to help justify the spend around compliance."

Jane Froyd,
SVP, General Counsel
America's Treasury Wine Estates

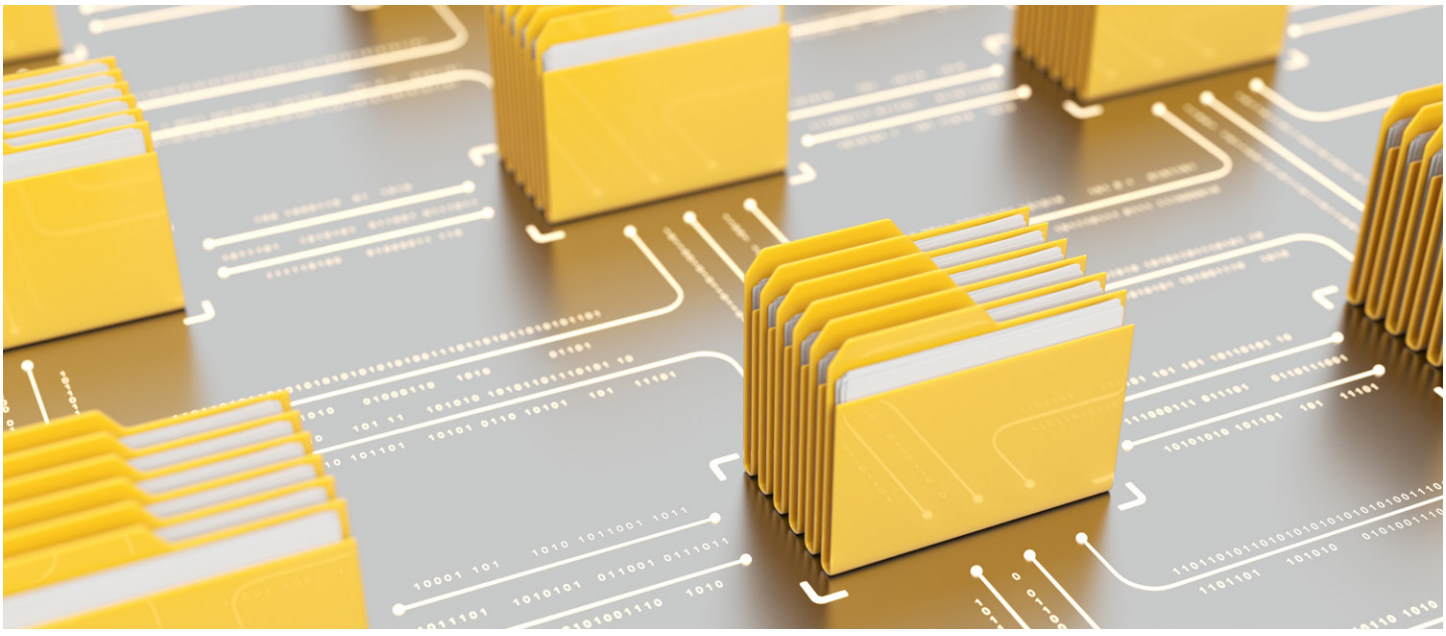
#2 Updating the Data Inventory

Think of a data map as a product, not a project. Like a product, it should be constantly evaluated, updated and assessed for quality. Failing to take this approach usually results in a data map becoming outdated before it provides any real value to the company.

- As mentioned above, having a defined, automated process can keep information coming in on a more consistent basis so that it doesn't feel like every update has to be its own time-consuming project.
- Another way to ensure the data map stays updated is to make sure that it is fully integrated with the company's HR and asset management systems so that the map reflects current employee and systems information.

"An essential component is understanding your retention obligations and how long do you have to maintain information? And that correlates to understanding the types of records that contain sensitive and personal data. That's how the CCPA was written when it comes to regulatory requirements for keeping records and information, and it's also how the business people think about their world, understanding how that information is collected, the various applications where that information could reside."

Rebecca Perry,
Director of Strategic Partnerships
Exterro



#3 An Incomplete Data Inventory

A common mistake organizations make with data maps is that they omit important information and therefore render the data map far less useful than it should be. Before any data mapping initiative gets off the ground, project organizers should assemble all the key stakeholders and gather feedback on what information needs to be included.

For example, a company's general counsel will want to make sure the data map includes retention schedules, litigation risk profile and accessibility constraints of particular data sources. Meanwhile, a chief privacy officer will likely want to know which data sources contain sensitive customer information that must be carefully protected. Understanding how different business units plan to interact and use the data map will help guide the information gathering and make the process of building the map far more efficient.

"So what the CCPA says is that for intentional violations, the State of California can pursue penalties up to $7,500 per violation. And I know from my former life as an enforcer, that the AG's office typically takes a very expansive view of a violation. So these penalties can get pretty stratospheric, pretty high. In the event of a data breach, where a company is found to have unreasonable allowed data to be both accessed and acquired by an unauthorized party, this law now provides for statutory damages ranging from $100 to $750 per data subject."

Jeffrey Rabkin,
Cybersecurity, Privacy, and Data Protection Partner
Jones Day

#4 Accounting for *ALL* Data Sources

For a data map to be effective, it has to be comprehensive. In today's digital world, that means it must account for things like mobile devices and cloud-based applications, including social media, since ESI from these sources is increasingly being sought in litigation. It is critical to identify how and by whom these sources are used and any relevant ESI that may exist on them (customer service records, marketing materials, etc.):

- In the case of mobile devices, it's important to identify any relevant data that is specific to the device versus that which can be accessed from a more traditional ESI source, such as an email server.
- When it comes to mapping social media use, it's imperative that the information be updated on a regular basis since usage trends tend to evolve very rapidly.

"I think that the challenge is really getting our arms around the data that we have and understanding where it lives, who's going to own the data and where it's shared. And then, as well as the logistics around how to handle these consumer requests that are coming in, how to validate them, how to respond to them, how to maintain records of that going forward."

Jane Froyd,
SVP, General Counsel
America's Treasury Wine Estates

CHAPTER SIX:

A Data Inventory Case Study

What does a practical case of building a data inventory look like? Jane Froyd, General Counsel for America's Treasury Wine Estates, recently spoke about her experience on an Exterro webcast.

"For a lot of us, data really lives and people oversee it across all different kinds of departments. And so, what was important for us is really to engage the business folks across the organization and make sure that they came together to talk through data and understanding what was collected, where it was living, with whom it was shared. And oftentimes, things that the legal department might assume about data just doesn't line up with reality.

We began our process with identifying key stakeholders across the business and to better understand their practices around data. And so that for us, it was folks not only in IT, but also in marketing, our direct consumer sales, to across the company. We started off with an initial ask for budget for outside counsel to work with us on updating our policies and terms and conditions, and doing that sort of initial data review.

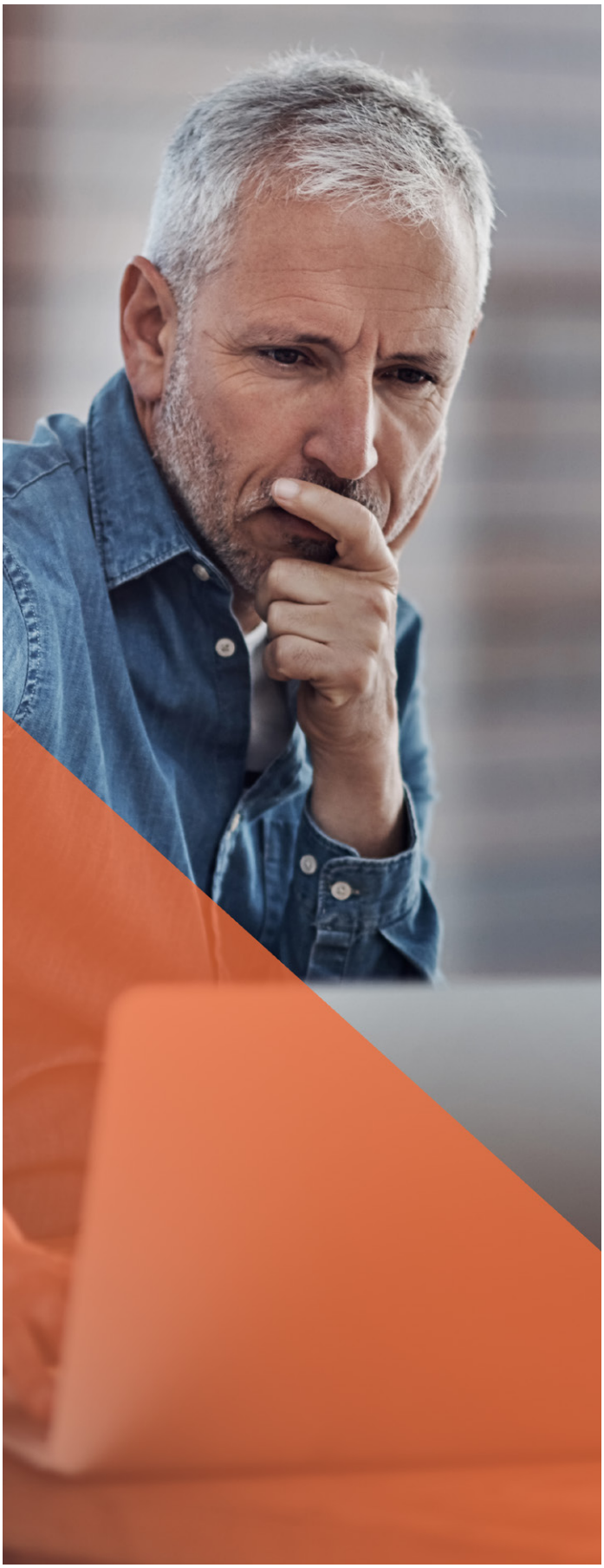
We started engaging outside counsel to help us assess, for our companies, the steps we would need to take. And what was clear initially, the first step we needed to take was getting our arms around the data that we have—knowing the volume of data, the types of data, how we're handling it—which helps us then to really assess the risk and plan for a budget.

So we put together a team. We were fortunate enough to have a good project manager to move the process along. We worked with [Exterro] to come up with a survey. They had a great template, and then we made it specific to our company. We identified who needed to fill out the survey of collecting information about data, and then enacted that process. Hounded people to complete the survey. Exterro helped us analyze it, and we were able to present on it to sort of an overall steering committee to determine next steps within about a month's period. So that's how we approached the data mapping analysis piece of the project.

The next step then is looking towards what kind of solutions we want for addressing the consumer requests and we did that through a process of looking at outside third-party possibilities as well as creating something internally. And then, we'll also be working through things like our third-party contracts to assess risk around that as well, but that's sort of how we've broken down the steps and are evaluating budget as we go along.

It's precisely what's driving our compliance roadmap. And frankly, it's helping us as a company also just step back and look at data governance more broadly, and how we might want to improve and build on what we've done so far in our thinking as a global company around data."

Jane Froyd,
SVP, General Counsel
America's Treasury Wine Estates



Conclusion

When it comes to new privacy laws like the CCPA—or any of the more than 25 laws being considered across the U.S. alone—having a robust and up-to-date data inventory is the first step in establishing compliance. The most defensible and accurate way to develop and maintain a data inventory is with Exterro's Data Inventory technology. Read more about how our platform can keep you ahead of the coming data privacy regulation onslaught, or ask for a demo.

LEARN MORE

GET A DEMO

exterro®

1.877.EXTERRO

www.exterro.com