The Best Data Retention Policy Template to Get You Started

Overview

Organizations of all sizes and industries benefit from a comprehensive data retention policy. Between a sprawl of cloud-based apps and industry guidelines and laws, outlining what data needs to be stored, how it needs to be stored, and how long it needs to be stored, is no easy feat. However, with the right data retention policy template, you’ll have a solid starting point.

In this whitepaper, we'll walk you through data retention best practices and provide you with a downloadable template to help you get organized and gain better visibility into your data’s lifecycle.
Before filling out our data retention policy template, you’ll want to do some preliminary work. A robust data retention policy is a living, breathing document — which means setting up a sustainable foundation is key. When meeting legal requirements and understanding the retention and discovery capabilities of your apps, your data retention policy should be flexible to an ever-changing, and rapidly growing data inventory. By following these steps, your data retention policy template will sustain your organization’s changes and growth for years to come.

Identify where your data lives and classify it

The first step in filling out a sustainable data retention policy template is identifying where your data lives. Make an exhaustive list of every app and data system in the cloud or on-premise that holds company data. Once you’ve done this, classify the types of data most pertinent to your organization. Organizing data that’s related to your industry is a good start. For example, if you’re in Healthcare, this might be PII such as dates of birth, social security numbers, and medical history, whereas if you’re in finance, this might be credit scores, PINs, or loan information.

Organizing your data retention policy in this way will not only help you parse out your most sensitive information first, but also highlight the data retention periods that automatically apply to you by law. Once your most sensitive data is categorized, it becomes easier (and less risky) to sort through the rest. We also recommend a data classification schema with categories such as “confidential”, “proprietary”, and “public.”

Understand which laws apply to you

Before filling out your data retention policy template, consult your legal and compliance teams closely. Legal requirements take precedence over business needs, and understanding which laws and regulations apply to your organization comes first. Sometimes, if more than one regulation applies to your organization their data retention requirements will conflict. In this case, you’ll want to outline what instances would create this conflict and document a plan of action for when the time comes.
Align your data retention policy with your compliance policy

Similar to legal obligations, your data retention policy should go hand in hand with your compliance policy. But compliance policies aren’t just about undergoing audits or maintaining CCPA compliance, they also extend to internal procedures that prevent risky or illegal activities. Creating a data retention policy with this in mind can serve as a proactive mechanism against risk. For example, if it’s against your organization’s compliance policy to share sensitive customer information, your data retention policy should reflect where that sensitive information lives, how long it should live there for, what its source’s default retention settings are, and how to retrieve it if necessary. Filling out your data retention policy template with this in mind will make all the difference for security, privacy, and overall information governance.

Learn the ins and outs of your data sources

All too often organizations make the mistake of setting data retention policies without getting to know the apps that hold their data. Until you understand the purpose of your applications and what their native capabilities and limitations are, you can’t set realistic data retention goals. Although it’s impossible to know every application like the back of your hand, you’ll want to get as much information as you can from the people that do: Interview employees and ask them how they’re using the system, contact vendors and ask detailed questions around retention and discovery capabilities, and when you’re done, document it all. Once you’ve done this, it becomes easy to spot and mitigate risk.

Outline when and how data should be archived or deleted

Once you know what data you have, where it lives, and what laws and policies pertain to it, it’s time to develop a retention period for it. Start with legal obligations — do you have to keep this data for one year? Five years? Seven years? Make sure that retention period is recorded and enforced. If you don’t have a legal obligation to retain data, work with stakeholders in other departments to get a holistic view of your data’s value. If there are no clear benefits to retaining it, ask yourselves, “What is the downside to deleting this?” or “Can this be archived?”

After a retention period is established, you should document the manner in which data should be deleted or archived. Will your applications delete data automatically or will it have to be manually done? Where will the data be stored if archived and how long should it stay archived for? It’s important to think about the answers to these questions when customizing your data retention policy template.

Monitor your policy regularly

Even after your data retention policy template is filled and complete, the work doesn’t stop there. A good data retention policy requires ongoing maintenance to provide continual value. Make sure you’re constantly monitoring retention updates to your current applications and adding the details of new ones early on in their implementation. Perhaps set a monthly or yearly check-in to ensure your policies are still adequate. Your data retention policies should never be outdated, so long-term thinking and process can help ensure it remains an enduring source of truth.
Now that you’ve covered all of your data retention bases, it’s time to put it in writing. We created this data retention policy template with all of the above considerations in mind and made it adaptable to your unique needs. Once again, it’s imperative that you consult your legal and compliance teams while filling this out. You also may also find that you need to pull in other key stakeholders such as HR, Finance, or IT throughout the process to make sure no stone is left unturned.

02.

How to use Onna’s Data Retention Policy Template

Now that you’ve covered all of your data retention bases, it’s time to put it in writing. We created this data retention policy template with all of the above considerations in mind and made it adaptable to your unique needs. Once again, it’s imperative that you consult your legal and compliance teams while filling this out. You also may also find that you need to pull in other key stakeholders such as HR, Finance, or IT throughout the process to make sure no stone is left unturned.

PART 1

The Retention Schedule

Go to the first tab of our data retention policy template to locate the retention schedule. This will be your central source of truth to address what data you retain, how long you retain it, and why.

PART 2

Retention & Discovery Overview for Cloud Applications

Go to the second tab of our data retention policy template to locate our retention and discovery overview for cloud applications. This section gives you a high-level overview of these apps’ native capabilities and limitations when it comes to data retention and eDiscovery. Chances are you already have a few of these apps in your tech stack, but if you don’t, feel free to add data sources and research of your own.
## Business Function
List the business functions that oversee critical data in your organization. We listed typical functions you can find at almost every organization, but depending on the size and structure of your organization, this column may look different. Feel free to add or subtract to this list and customize labels.

It’s important to note that sometimes responsibility over certain data may be shared by two business functions. If this is the case, make sure that is reflected in record class names and/or notes.

## Record Class Name
Label your record class. The record class name is the type of file you are saving within each business function. There can be multiple files to save within each business function, so be sure you assess their retention periods individually. It may even make sense to create sub-groups of your record classes. For example, in human resources, you can break up files into a benefits category as well as an employment category.

We’ve included some typical record classes for reference.

## Record Class Code
Within record classes are record class codes to help organize data even further. Regardless of whether your record classes are saved in the cloud, on a hard drive, or a data room states away, you want to classify them according to a specific code to communicate to stakeholders what the retention requirement is. Note: Certain record classes may belong to more than one business function. For example, your compliance, audit, and IT teams may have to collaborate on a security audit. Regardless, make sure you stick to one code for that record class.

## Retention Period
Input the retention period for the corresponding record class. Remember, always take legal requirements into consideration first. If there are no legal requirements, consider business needs, then operational efficiency to determine what to retain or delete. Again, keep in mind there may be different retention periods for different record classes. Assess them on an individual basis.

<table>
<thead>
<tr>
<th>Business Function</th>
<th>Retention Citation</th>
<th>Data Sources</th>
<th>PII Documentation</th>
<th>Authorized Manager</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the business functions that oversee critical data in your organization.</td>
<td>If applicable, link to the citation that is driving the retention period.</td>
<td>It's so important to document where the data within each record class lives. This way, you'll know exactly where to collect data from in the case of litigation, data subject access requests, or any matter thrown your way. Tip: The second tab of our data retention policy template will dive deeper into retention within data sources.</td>
<td>Check the box if the corresponding record class contains PII. By taking note of which record classes contain PII, you can better respond to sensitive privacy matters down the line.</td>
<td>Ask yourself, who is authorized to retain, delete, or archive data? Assign this person(s) as the authorized manager. They will oversee the entire lifecycle of their respective record classes.</td>
<td>Use this column to jot down any information you feel is relevant to know about the corresponding record class. Is there a specific way this data needs to be archived or deleted? Is there a limitation in the data source that requires regular maintenance? Any knowledge like this could be helpful to keep on hand.</td>
</tr>
</tbody>
</table>
PART 2  Retention & Discovery Overview for Cloud Applications

Cloud Communication App
Here, we've listed some of today's most popular cloud collaboration/communication apps. This is not an exhaustive list; however, we focus on the apps that we've found present the most challenges for data preservation and discovery and felt would be helpful to analyze.

Data Types
In this column we've listed the data types we believe are worth preserving within each app. You may add or subtract to this list based on your individual needs, but what we've listed we feel are necessary to preserve.

Native Retention Settings
Here’s a breakdown of each app’s native retention settings and any limitations we know of. It’s important to note that new updates are being made all the time. Be sure to check in with your admin and the vendors themselves to get the latest updates and understand how your organization’s plan stacks up to legal and compliance requirements.

Native eDiscovery Method
Here’s a breakdown of each app’s native eDiscovery methods and any limitations we know of. It’s crucial to have an eDiscovery method in place to help you find and take action on data at a moment’s notice. Tip: Onna eDiscovery is compatible with all of the apps you see on this list.

Like this template?
Want to see how Onna can help you control data retention in today's most popular cloud apps?

Reach out to learn more