CHECKLIST: Setting up a DSAR process

IDENTIFY THE MAJOR STEPS THAT ANY BUSINESS SHOULD CARRY OUT TO DEVELOP A SCALABLE DSAR WORKFLOW

DEFINE YOUR POLICY

Before you start building your DSAR program, you'll need to define your policy. Essentially, you need to formalize your process, make a plan for how you'll handle DSAR requests, and communicate that policy to your customers and employees.

☐ **Determine how you will handle different types of data**

Different data privacy laws will have different standards, but if you want your DSAR program to have broad coverage, you'll need to determine your policy for:

1. Consumer data, which is the most commonly regulated type of data you'll collect
2. Employee data, which can become voluminous during an employee's tenure
3. Candidate data, which often contains sensitive information
4. Special category data, which requires special treatment due to its sensitive nature

Review the laws that apply to your organization or that you wish to become compliant with and see what specific requirements they have for these different types of data. Once you have an understanding of your requirements, codify them in your policy.

☐ **Decide whether you will handle DSARs by jurisdiction or default to the strictest law**

Not every law has the same requirements for DSARs. Under the CPRA, for instance, DSARs are due within 45 days, while the GDPR has them due in 30 days. The rights that consumers can act upon vary from law to law slightly as well.

Some businesses choose to follow the process required by the data subject's governing law, while others apply the most comprehensive law in every circumstance. The former approach can minimize your effort in certain respects, while the latter minimizes your risk.

☐ **Decide whether you will fulfill DSARs regardless of where the data subject is located**

You don't have to fulfill DSARs if the data subject is located in a jurisdiction that lacks a data privacy law mandating DSARs. Executing only those DSARs that come from covered jurisdictions can cut down on your workload, but it can also make some consumers feel less important than consumers from, say, California. It can also increase the risk of accidentally refusing a valid DSAR if you should mistake a consumer's geolocation.

☐ **Identify the responsible parties for your DSAR process**

Define which roles or individuals are responsible for different parts of the DSAR process. You might find it useful to assign responsibilities to roles like:

- The privacy leader: Who will be responsible for the overall effectiveness, budgeting, and strategy of your privacy program?
- The DSAR process manager: Who will administrate, oversee, and manage your DSAR process, both in general and on a case-by-case basis?
- Data store owners: Who is in charge of the different data stores where consumer data can be found across your organization? These individuals will need to know that a part of their responsibilities is the fulfillment of DSAR requests that involve information within their data store.

☐ **Define your data retention schedule**

How long will you retain different types of data? The more data you hold on to, the more work you'll need to take on to execute a DSAR, and the greater your risk.

Look at the purpose behind your data collection as outlined in your privacy policy. You might collect personal information for marketing purposes, for instance. In that case, you could delete contact information from individuals who haven't engaged with your organization in the last six months. For email data, you could adopt a blanket policy to delete all archived emails after a year has passed. What's important is that you eventually delete or de-identify data rather than hold on to it indefinitely.

LAY THE FOUNDATION

Before you can start acting on DSAR requests, you'll need the right foundational elements in place. These steps will ensure you're set up for success.

☐ Make a data inventory

Efficiently executing a DSAR request requires that you know where different types of consumer data lives across your organization, where it's transferred to, and what is done to it. Create a document that records this information, and update it on a regular basis. A good way to approach this exercise is to use the GDPR's guidance on Records of Processing Activity (RoPA).

☐ Reach out to outside organizations that process your consumers' data

Certain data privacy laws require you to pass along DSAR requests to any vendors or third parties that handle your consumers' data. That could include, for instance, ad tech companies, consultants, and the like. Make sure you contact the individuals responsible for privacy at those organizations to align on expectations and processes.

☐ Develop a means for data subjects to submit a request

Some businesses use a form to accept DSAR requests, while others use an email address. Note that many data privacy regulations require you to accept DSARs regardless of the channel they are made through.

Whatever method you choose, it's essential that you spend time thinking about how to make the ingestion of DSAR requests easier. The more manual this process is, the more time-consuming it becomes and the easier it becomes to make mistakes. In Osano, you can allow data subjects to make requests via form, email, or even over the phone. This way, you can centralize all of your DSAR requests in the Osano platform while still providing data subjects with a variety of channels to make their requests.

☐ Develop a means of verifying requests

You can't just give out an individual's data to anybody who claims to be that person; instead, you need to ask for identification to verify the request you receive.

Generally, data privacy laws require you to ask for as little information as possible to verify the request. After all, this is yet more personal information that your organization is collecting and will need to be responsible for. Photo IDs, for instance, should only be used for deletion requests or for requests that involve sensitive personal information.

EXECUTE DSAR REQUESTS

With a solid foundation in place, you're ready to actually execute a DSAR request. Here's how you should approach the fulfillment of a DSAR request.

☐ Accept the request

Whether you use a form, email address, a combination of the two, or another method altogether, you'll want to promptly review incoming requests. If you're using Osano, you'll receive automatic notifications about new incoming requests.

☐ Acknowledge and verify the request

Using the method you developed previously, verify the data subject's identity.

Let the data subject know that you've received the request and are working to fulfill it—most data privacy laws require that requests be fulfilled within 30 or 45 days. Ideally, you can conduct this communication through a secure portal. That way, you don't accidentally create yet more consumer data to be managed in other email or messaging systems.

In Osano, data subjects are able to upload the proof of identity that you specify, whether that's a photo ID, employee badge, or another form of identification. What's more, all DSAR comms live within the Osano platform, making it easy to keep track of the personal information you collect when pursuing compliance.

☐ Coordinate with responsible data store owners

If you're adhering to security best practices, then you won't have access to every data store in your organization; only the people who need regular access to those data stores will have access. That means you'll need to notify those data store owners about the relevant DSAR task they need to complete.

That could be updating certain data fields, deleting data, summarizing the data, and the like. If you're using Osano, some of these tasks can be automated, ensuring that you don't have to wait for a busy human to get around to it. Certain tasks are not appropriate for automation, however, and a human should always review any changes for accuracy.

Whether the task is automated or not, Osano automatically notifies and reminds data store owners when they have DSAR tasks they need to complete or review. Without a platform like Osano, it'll be incumbent upon the DSAR process manager to communicate what needs to be done and when.

☐ Communicate results to the data subject

Once you and your colleagues have completed the tasks associated with the DSAR, you'll want to communicate the results to the data subject.

This might be a simple confirmation that the task has been completed, such as would be the case for deletion requests. For summaries and other requests that require a deliverable, data privacy laws require that you deliver the data in a portable format—that is, a format that's easy to open, use, review, manage, and so on. If you deliver data in a variety of difficult-to-use formats, you'll be out of compliance.

MANAGE THE PROCESS

It's not enough to build a robust process and leave it alone; part of what makes a DSAR process sustainable is regular maintenance and management. Here are the steps involved.

☐ Record DSAR fulfillment

Anytime you complete a compliance activity, it's a best practice to record that completion. DSARs are no exception.

You may do everything to the letter, and a data subject still might file a complaint with a data protection authority because they're misinformed about their rights, are simply trying to be vexatious, or for any other reason. Or, a data protection authority might feel the need to investigate your organization for some other reason. In any case, if you record the fulfillment of the DSAR, you'll be able to demonstrate compliance. Often, data privacy laws require this.

Plus, recording information like the time it took to complete certain requests, whether any challenges were encountered, and similar metrics can help you improve your DSAR process in the long run.

☐ Review feedback

Everyone involved in the DSAR process—from the data subject to data store owners—may provide valuable feedback that can help identify gaps and inefficiencies in your DSAR program.

The data subject, in particular, can be an important source of feedback. If the experience is unpleasant for them, they may file a complaint with data protection authorities. Even if your process is compliant, if it regularly leaves data subjects feeling frustrated, then you may face interruptions to your business and unwanted attention from authorities.

☐ Sync your DSAR process with your RoPA

If you're following the advice in this checklist and are keeping a RoPA, then you'll want to make sure that changes in your DSAR process are reflected in your RoPA and vice versa. A RoPA should be a regularly updated snapshot of your data processing activities. If you add new data stores, collect new data, or do anything new that you need to account for in your DSAR process, then you'll want to make the corresponding change to your RoPA.

☐ Learn and iterate

It's unlikely that you'll have the perfect process in place on your first try. As you process more DSARs and record your findings, periodically review the process as a whole and see how it can be improved. Maybe your organization has added new systems for data collection and storage since you last changed your DSAR process; maybe you've identified a more secure and centralized way of storing certain categories of data; or maybe you've outgrown using email and spreadsheets to manage the process.

Whatever opportunities you identify, remember that your DSAR process shouldn't be a one-and-done effort. Rather, it's a living part of your overall compliance program.

STREAMLINE YOUR DSAR WORKFLOW WITH OSANO

As your DSAR program matures and your business grows, it'll become more and more important to have a DSAR workflow that scales efficiently.

Osano's Subject Rights Management and Data Discovery work together to streamline the most tedious tasks and biggest sources of risk in your DSAR program, including:

- Securely communicating with data subjects to accept DSARs, verify identities, and transfer data
- Automatically identifying relevant data in connected data stores
- Notifying and reminding data store owners about DSAR tasks they're assigned to
- Automated summaries and deletion of data
- And more

SCHEDULE A DEMO

osano

@osano
linkedin.com/company/osano
http://facebook.com/osanoatx

osano.com

About Osano
Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 website to capture consent for more than 2.5 billion monthly visitors.