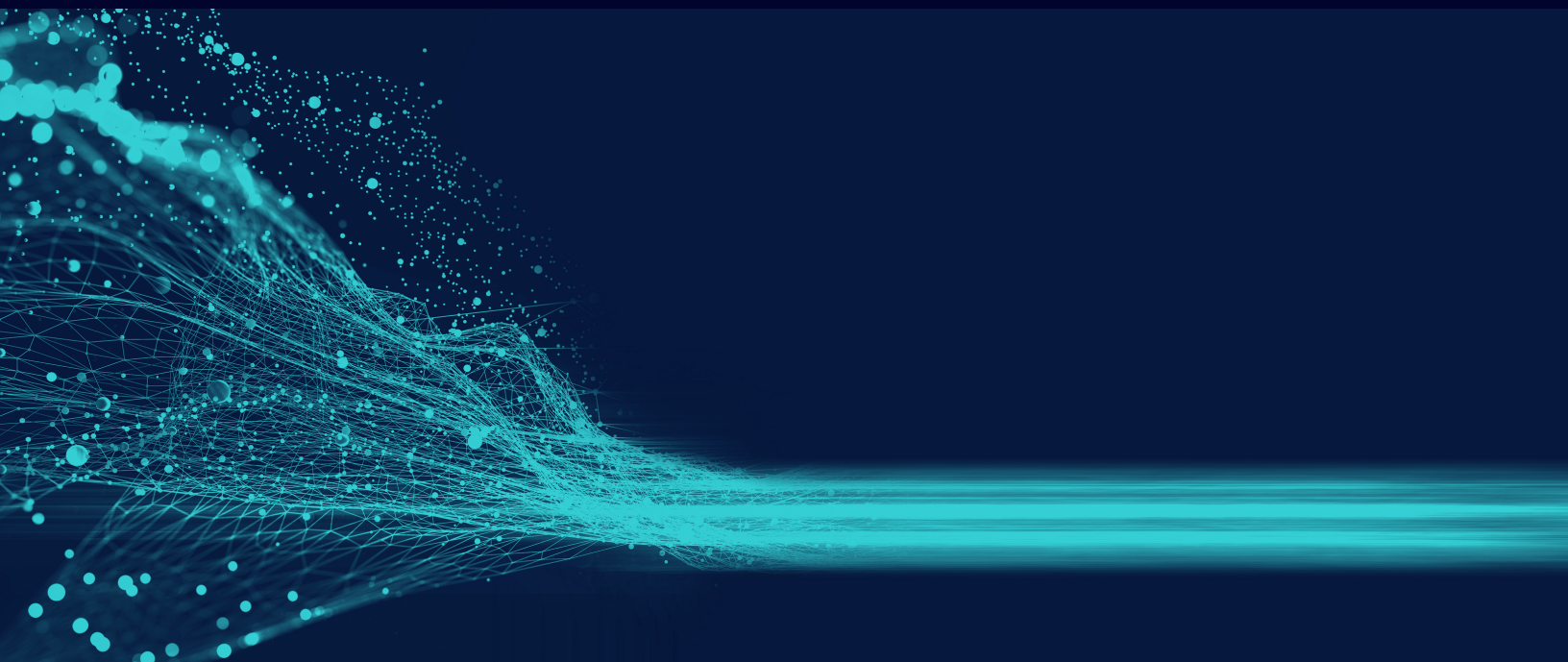
WHITE PAPER

RELYANCE AI

Understanding Data Subject Access Requests & How to Choose the Right Solution

Although the DSAR fulfillment process should be straightforward and simple, current tooling makes the process impossible to perfect. Avoid the resource burden by learning what's wrong with solutions today and what to look for in the future in order to manage DSAR volume at scale for global compliance.



Background

Certain data subjects now have the right to exercise control over their personal information. This is a core element of most data protection laws throughout the world. While the specific rights vary from regulation to regulation, they generally center around a few key concepts: the right of a data subject to be informed about how her personal data is collected, used and/or disclosed; the right to correct inaccuracies in her data; and the right to control or influence the manner in which her data is processed. Data subjects may exercise their rights via actions commonly referred to in the privacy community as Data Subject Access Requests, or "DSARs". DSARs have become some of the most high-profile scrutinized elements of data governance and privacy compliance, and have drawn the focus of the public along with regulators. Failure to accurately and completely respond to DSARs may result in severe penalties, including reputational and financial–in some cases up to 4% of an organization's annual gross revenue.

As new data protection laws emerge, organizations that process personal data for their business operations are required to manage an increasing number of compliance obligations, procedural considerations, and the demands of an ever-more privacy conscious public. One of the most commonly reported pain points among those organizations is the difficulty in managing DSARs at scale. They struggle to receive, manage, and respond to DSARs accurately and within the time period required by applicable law.

Technology has not yet come to the rescue. Despite the wide array of privacy rights management tools available today that are marketed as solutions to the DSAR problem, most lack the features necessary to deliver an automated solution that works at scale: integration with a continuously-updated data inventory and map, automated workflows, and built-in guidance on how specific DSARs should be processed. This paper will explore the current state of data subject rights and DSARs today, why most DSAR management solutions fail to promote true compliance with data protection regulations, and what organizations should look for in a DSAR management and data governance solution that can manage DSAR volume at scale and in compliance with applicable laws.

The State of DSARs Today

Organizations have experienced a significant increase in the frequency and visibility of DSARs in recent years, particularly since the passage of a number of high-profile data protection regulations: the General Data Protection Regulation 2016/679 (GDPR) in the European Union, the California Consumer Privacy Act (CCPA)[1] in the State of California, and the General Personal Data Protection Law 13709/2018 (LGPD) in Brazil.

These new regulations have led to a sea change in the data protection environment, as they all feature two significant components: extraterritorial reach and the creation or expansion of data subject rights. Now, many organizations must account for DSARs that emanate from all over the world under differing regulatory frameworks. Specifically, organizations must respond to DSARs exercising the following data subject rights under those aforementioned laws, while navigating each law's requirements for response time and content, along with any restrictions.

Under the GDPR, individuals in the the European Economic Area[2] may issue DSARs to organizations subject to the GDPR throughout the world[3] to exercise any of the following rights:

- The right to receive information about her personal data being processed, as well as a copy of that data
- A data subject may have inaccuracies related to her personal data corrected
- The right, under certain circumstances, to require the organization processing the data subject's data to delete her data (also known as the "right to be forgotten")
- Where an organization is processing personal data based on the consent of the data subject, the data subject may withdraw her consent
- In some situations, a data subject may restrict the processing of her data to some purposes
- A data subject may request that her data be provided to her or another organization in a usable format
- A data subject may object to certain types of processing, after which the processing activity must cease

---

1 The State of California recently passed the California Privacy Rights Act of 2020, which will go into effect January 1, 2023, amending the CCPA and, among other items, adding a number of additional data subject rights.

2 The European Union, Norway, Iceland, and Liechtenstein.

3 See GDPR Articles 15 - 18, 20 - 21.

Pursuant to the LGPD, data subjects in Brazil may issue DSARs to organizations subject to the LGPD to exercise the following rights[4]:

- The right to access data
- The right to correct inaccurate, incomplete, or out-of-date data
- The right to force the anonymization, blocking or deletion of data under certain circumstances
- The right to port data to another organization
- The right to withdraw consent, and to force the deletion of any data processed on the basis of the data subject's consent

Lastly, the CCPA affords California residents the right to issue DSARs exercising the following rights[5]:

- The right to request a record of the personal information an organization holds about the data subject and how that information is used
- The right to force an organization to delete the data subject's personal data
- The right to opt-out of having a data subject's data sold to third parties

In addition to the foregoing regulations, data protection laws affording some degree of data subject rights exist in countries throughout the world, including much of Latin America, Canada, China, South Korea, Japan, and at the U.S. state and federal level[6]. Therefore, competent DSAR management has become a critically important compliance and risk management tool for organizations of all sizes throughout the world. However, many organizations struggle to maintain compliance with their varying obligations under applicable laws. In a recent survey, more than half of the California privacy professionals surveyed reported that DSARs are the hardest part of maintaining compliance with the CCPA.[7]

---

4 See LGPD Article 18.

5 See CCPA § 1798.100, 1798.105, 1798.120.

6 While the United States does not have a generally-applicable data protection regulation, it has a number of sector-specific federal privacy rights that afford data subject rights, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair Credit Reporting Act (FCRA), and the Family Educational Rights and Privacy Act (FERPA).

7 See "Study Highlights Data Subject Request Volum, Spending under CCPA" by Ryan Chivetta for the International Association of Privacy Professionals, available at https://iapp.org/news/a/study-highlights-data-subject-request-volume-spending-under-ccpa/ (as of August, 2021).

Live Data Maps and Inventories are Key to Any Successful DSAR Tool

To date, many organizations have attempted to manage DSARs via ad-hoc internal processes or vendor tools that either cannot handle large DSAR volume at scale, or, more commonly, prevent organizations from responding to DSARs accurately due to a failure to account for an organization's full data inventory and data flows. In order to effectively manage DSAR volume, organizations must start from a simple, yet critical, foundation: an accurate understanding of what personal data the organization possesses, where it resides, and with whom the organization has shared it.

Once an organization receives a valid DSAR, it must first take a few key steps: identify what personal information the organization has on the data subject across all departments and processing operations, identify where that data resides, and identify which of the organization's vendors are processing that subject's personal information. If the organization does not have full visibility into each of those three items, they will either fail to respond to the DSAR within the timeframe required by applicable law, or fail to identify all of the personal information within the scope of the DSAR, resulting in an incomplete response potentially in violation of data protection law.

DSAR tools lacking integration with continuously updated data inventory and maps wil also fail in any of the following three key areas:

Data Lifecycle Management

In order to determine the personal information that falls within the scope of a DSAR response, organizations must have a clear understanding of their data assets as they progress through the entire data lifecycle, from ingestion, to processing, to destruction. In addition, organizations must know which of their data assets are being used in their various processing operations, otherwise, the scope of their search for responsive data is likely to fail to include all relevant data repositories and/or processing operations.

Cross-functional Data Management

As many privacy professionals understand all too well, individual departments within organizations tend to fail to keep other departments, particularly those responsible for legal compliance and privacy, updated on changes to their data inventories or processing operations. This disconnect sets most organizations up to fail when managing DSARs, as it does not account for cross-functionality and prohibits an effective, centralized approach to DSAR response that can discover all the personal information of the relevant data subject. DSAR management solutions will similarly fail unless they are integrated with a live data map accounting for all of the organization's data assets.

Processor Management

One of the crucial workflows required for a compliant DSAR response is identifying which of the organization's vendors process the personal information of the data subject on the organization's behalf. A number of data subject rights, including the right to deletion and the right to rectify inaccuracies in personal data, cannot be fulfilled unless the organization receiving the request passes it on to its vendors, who must also honor the DSAR. In order to successfully do so, the organization, or the DSAR management solution it uses, must have a live, up-to-the minute look at which of its vendors are processing the personal data of the data subject. Otherwise, the organization risks non-compliance with applicable law for failure to account for all personal data within the scope of the data subject's DSAR.

Why Artificial Intelligence and Machine Learning Are Required for Any DSAR Solution to Operate Effectively and at Scale

While this paper has established the importance of live data inventories and maps in supporting DSAR workflows, the time and effort necessary to create and maintain them is often unmanageable. As most privacy professionals know, maintaining data inventories and maps is a labor-intensive task that requires constant upkeep and consistent collaboration with cross-functional teams across the entirety of an organization. Even the best privacy teams will be limited by bandwidth, the responsiveness of their coworkers, and the insights they are given into their organization's data lifecycle.

In addition, privacy teams that can devote the time necessary to maintain world-class data governance often struggle with another important element of DSAR compliance - determining the exact content of their DSAR response. Data protection laws generally set disparate requirements as to what exactly must be included in responses to various DSARs, and restrictions on information that must be excluded, such as the personal data of other data subjects that is intermingled with the data of the data subject that issued the DSAR. Privacy teams regularly struggle with the challenge of both understanding the DSAR requirements and restrictions under various data protection regulations, and understanding where and how to apply them to each individual DSAR their organization receives.

Artificial Intelligence (AI) and Machine Learning (ML) can help. As AI and ML tools continue to mature, they can be leveraged to solve the most pressing problems organizations face in complying with their DSAR obligations under applicable law. With minimal implementation and effort, the Relyance AI Platform automatically creates and maintains a live and continuously monitored inventory and map of your organization's data assets, and offers an integrated DSAR management solution that draws from that inventory to automatically evaluate incoming DSARs, manage the data collection workflow within your internal data assets and with your vendors, and produce compliant DSAR responses.

Conclusion

DSAR management remains a major compliance hurdle for even the most sophisticated companies and privacy teams. The Relyance AI Platform provides an AI- and ML-powered solution that, through its integration with your organization's live data inventory and map in the Platform and built-in guidance, provides an out-of-the-box solution to manage your DSAR inflow both at scale and in compliance with applicable data protection regulations.

RELYANCE AI