ALM | LAW.COM

Legaltech® news

What DSARs Reveal About an Organization's Data Maturity

By Esther Birnbaum and Christopher Wall
October 28, 2026

The Conversation Around DSARs Has Changed

Legal departments have traditionally viewed data subject access requests (DSARs) as privacy compliance obligations. But responding to a DSAR can also reveal how well an organization's data governance practices actually work.

As organizations distribute information across cloud applications, collaboration platforms, mobile devices, and AI-enabled systems, responding to a DSAR requires much more than knowledge of applicable privacy laws and regulations. Organizations must know what personal data they hold, where it resides, who is responsible for it, and how it should be handled.

Recent research underscores growing demands on privacy teams. DataGrail's "2026 Privacy and AI Trends Report" found that overall data subject request volumes rose for the fifth consecutive year, although access requests declined overall and trends varied by industry. Professional services companies, for example, received 4.6 times as many DSARs as the average company in 2025.

At the same time, Cisco's "2026 Data and Privacy Benchmark Study" found that 65% of surveyed organizations struggle to access relevant, high-quality data efficiently. Together, these findings highlight the operational challenge: organizations face growing demands to manage personal information even as many struggle with



Courtesy photos

Esther Birnbaum, left, and Christopher Wall, right, with HaystackID.

data visibility and accessibility. DSARs provide a practical opportunity to evaluate how well those governance capabilities work.

Why DSARs Are Becoming More Complex

Part of the challenge is where information now lives. Business communications are spread across email, messaging platforms, cloud applications and other systems, making it harder to locate all the information relevant to a request. Relevant information may be embedded in documents, conversations, attachments and AI-generated outputs across numerous systems. AI-enabled systems can also raise questions about whether prompts, outputs, and interaction histories con-

tain personal data and how those records can be located. Employment-related DSARs can be especially demanding because responsive information may span human resources records, internal communications, performance evaluations, and workplace investigations.

At the same time, a request may implicate multiple business functions. Privacy professionals interpret each request and coordinate the response. Legal teams evaluate possible exemptions, privilege, third-party rights and litigation risk. Information security and IT teams help identify systems and preserve access controls. Human resources may hold key employment records. Business owners provide context that cannot be inferred from a search result alone. Regulators and data protection authorities continue to emphasize transparency, accountability, and timely response obligations.

Fragmented data and disconnected workflows can complicate DSAR compliance. For response teams, these challenges make it harder to establish complete search coverage, apply consistent review standards and document a defensible process.

Although the governing requirements vary by jurisdiction, an effective response commonly requires an organization to identify responsive personal data, evaluate applicable limitations or exemptions, protect the rights of others, and respond within prescribed time frames. The quality of that response depends on the underlying governance system, not simply the privacy team's understanding of the law.

What a DSAR Reveals About Data Maturity

A DSAR requires an organization to put its governance processes to work under real legal deadlines. A request may be completed through extraordinary manual effort, but that alone does not demonstrate a repeatable governance capability. A data map is useful only if it accurately identifies the systems containing personal data. A retention schedule is meaningful only if records have been retained or disposed of consistently. A review protocol is defensible only if the organization can show that it was followed. Viewed through this lens, a DSAR tests whether an organization can:

1. **Know** what data exists
2. **Find** where it resides
3. **Understand** what it contains
4. **Govern** how it should be handled
5. **Act** within required timelines

A DSAR can expose problems that aren't always apparent until an organization has to respond to a request. The team may discover a data source missing from its inventory or encounter large volumes of outdated or duplicative records that raise questions about retention and defensible disposition. It may also be unclear who owns a particular system or who is responsible for making decisions. Delays in getting input from legal, human resources, security, or business teams can reveal weaknesses in how those groups coordinate.

The difficulties encountered during a DSAR can be just as revealing as the final response. They show organizations what needs to be fixed before the next request, investigation, or dispute.

Turning DSAR Findings Into Better Governance

Identifying these weaknesses is only the first step. The bigger opportunity is to address the underlying problems rather than work around them each time a new request comes in.

Organizations can use what they learn to:

- Update data inventories and clarify ownership of information sources
- Refine retention, defensible disposition and data minimization practices
- Address weaknesses in governance controls and response processes
- Establish clearer responsibilities and escalation procedures across teams
- Evaluate whether improvements strengthen both compliance readiness and broader governance maturity

Data governance teams should therefore see each DSAR as a "probletunity": a challenge that simultaneously creates an opportunity to identify governance weaknesses, test existing processes and methodologies and improve operational readiness.

Metrics That Turn DSARs Into Governance Intelligence

Tracking the number of completed DSARs isn't enough to understand how well the process is working. Organizations should also look at where time is spent, which systems cause delays, and what repeatedly requires escalation. These are often the issues that point to larger problems with data governance.

A practical measurement framework may include:

- **End-to-end response time**, including time spent in intake, collection, review, approval and delivery
- **Data-source coverage**, including the percentage of known systems assessed and the number of previously unidentified sources discovered
- **Collection method**, including the proportion of material collected through automated, repeatable methods rather than manual intervention
- **Review effort**, including hours, volume, and the categories of issues requiring specialist judgment
- **Data reduction**, including duplicate, redundant, or nonresponsive material removed before substantive review
- **Third-party protection**, including the time and effort required to redact or de-identify information relating to other individuals.
- **Escalations and exceptions**, including the frequency and cause of privilege, exemption, identity, scope, or deadline issues
- **Supplemental work**, including missed-source corrections, follow-up searches, and post-production remediation
- **Improvement actions**, including ownership and closure of data-mapping, retention, workflow, or control gaps identified during the response

These measures are important, but none should become an end in itself. The purpose of these metrics is to identify patterns and to direct attention to the causes of delay, cost, and risk. If the same repository repeatedly requires manual collection, for example, then the appropriate response may be a technical integration, a clearer delineation of responsibilities, or a change in retention parameters. If review effort is driven by excessively duplicative content, data hygiene and defensible disposition may offer more value than simply adding reviewers. Tracking whether these issues recur across requests can also show whether governance improvements are actually working.

Scaling DSAR Response With Automation and Human Oversight

While AI-enabled systems create new governance challenges, AI-assisted tools can also help organizations manage DSAR volume by accelerating collection, classification, and review. These capabilities can reduce repetitive work, improve consistency, and help response teams focus on the material that most requires judgment.

Defensibility, however, depends on more than speed. Decisions involving privilege, legal exemptions, third-party information, identity verification, disputed scope, or potential litigation exposure may require contextual analysis and an accountable human in the loop. AI-assisted outputs also require validation appropriate to each use case, the potential risk and consequences of error, and the organization's documented methodology.

Depending on the application, validation may include representative sampling, targeted quality checks, and additional scrutiny of higher-risk determinations. The objective is not to require the same level of human review for every decision, but to establish a defensible methodology

for evaluating and relying on AI-assisted results. The question is where human involvement is most important. Technology can handle repetitive tasks and identify potential issues, while legal and privacy professionals focus on validating results, resolving exceptions and making decisions that require additional judgment. Human oversight is part of what makes the process defensible, not something that necessarily slows it down.

This combination of technology and human expertise also supports transparency. An organization should be able to explain what technology was used, what decisions it supported, how outputs were tested, where human review occurred, and how exceptions were escalated.

Organizations should evaluate AI not solely by how much review effort it eliminates, but also by how reliably it supports defensible, consistent, and auditable decisions.

The Organizational Payoff Beyond Efficient DSAR Responses

The benefits of getting DSAR response right extend well beyond privacy compliance. The same processes used to locate, collect, and review personal data are important in litigation, internal investigations, regulatory inquiries, cyber incident response, records management, and AI governance.

For that reason, DSAR improvement should not be treated as a narrow privacy project. For example, a data map improved after a DSAR can help teams identify relevant sources more quickly in litigation or cyber incident response. Clear ownership accelerates decisions. Consistent retention reduces unnecessary volume. Repeatable collection and review methods support quality and auditability.

Governance improvements made after a DSAR response can reduce the cost and complexity of future requests, regardless of their source. They can also make the organization better prepared for events in which the timeline is shorter, the stakes are higher, or the information environment is under greater scrutiny.

Beyond the Response

A DSAR remains a legal obligation, and timely, accurate compliance must remain the immediate priority. But the work should not end when the response is delivered.

Organizations can use recurring issues, process metrics, and post-response findings to move beyond reactive request handling, strengthen governance, focus investment, and improve readiness for a wider range of legal and operational demands.

Every DSAR should result in answers for the requester. But it should also produce answers for the responding organization itself. The real value comes from using those answers to strengthen data governance across the organization, not simply to make the next request easier to handle.

Esther Birnbaum *is executive vice president of legal data intelligence at HaystackID, where she leads initiatives integrating AI into legal technology, eDiscovery and compliance workflows. Previously, she served as associate general counsel at Interactive Brokers, overseeing eDiscovery and responses to litigation and regulatory investigations. Her expertise spans AI, privacy, information governance and complex litigation.* **Christopher Wall** *is data protection officer and special counsel for global privacy and forensics at HaystackID. He advises clients on cross-border privacy, data protection, cyber investigations and eDiscovery. Previously with Ernst & Young, Wall led complex international cybersecurity and discovery investigations. He holds certified information privacy professional credentials for the United States (CIPP/US) and Europe (CIPP/E).*

Reprinted with permission from the October 28, 2026 edition of the LEGALTECH NEWS © 2026 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or asset-and-logo-licensing@alm.com. # LTN-10292026