ENTERPRISE RESOURCES

DSAR Readiness Checklist For Google Workspace

Navigating a Data Subject Access Request (DSAR) is a major responsibility for any Google Workspace administrator. It’s a complex, multi-step process that can be a source of stress and compliance risk. The key to success isn't luck, it's a clear, repeatable plan.
This checklist is your definitive guide to DSAR readiness. It will help you assess your current capabilities, identify gaps, and ensure your organization is prepared to handle any request with confidence.

1. Governance & Responsibility

- □ You have a designated DPO or compliance officer responsible for DSARs.
- □ You’ve defined and documented a DSAR process, including intake, verification, review, and response.
- □ You’ve established roles and responsibilities between legal, IT, and HR teams.
- □ Your staff has received training on DSAR handling and data privacy obligations.

2. Discovery Capabilities

- □ You can search across all Google Workspace services: Gmail, Drive, Calendar, Contacts, Chat, Groups.
- □ You can identify personal data by keyword, label, owner, date, or other metadata.
- □ You can locate shared files, including externally owned documents shared into your domain.
- □ You can identify indirect identifiers (e.g., IP addresses, login metadata, browser activity) when required.

3. Access & Review Controls

□ You have a system for previewing content before exporting it.

□ You can request access to user data securely (e.g., with an approval workflow).

□ Your solution supports role-based access to sensitive data (e.g., IT vs Legal vs DPO).

□ There is a change approval or escalation process for unlocking or modifying sensitive data.

4. Export & Response Capabilities

□ You can generate clean, structured exports with only the relevant personal data.

□ You avoid exporting entire email inboxes or shared drives unless required.

□ You can exclude irrelevant, internal, or privileged information during the export.

□ Your exports include context (e.g., timestamp, access history, sharing settings) when needed.

5. Logging & Compliance

□ Every DSAR-related action is fully logged (who accessed what, when, and why).

□ Your logs are immutable and auditable, in case of regulator review.

□ You can produce evidence of DSAR fulfillment within required timeframes (e.g., 30 days for GDPR).

□ You can demonstrate that data integrity and security were preserved during the process.

6. Tools & Automation

- □ You use automation to reduce manual DSAR handling (e.g., templates, workflows).
- □ You've integrated your DSAR process with existing ticketing systems or intake forms.
- □ You use tools (like GAT+, GAT Unlock, or similar) that go beyond Google Vault.
- □ You've tested your DSAR process at least once in the past 12 months.

7. Timeliness & SLA Tracking

- □ You have a system to track DSAR request deadlines and internal SLAs.
- □ You can generate status reports for ongoing or completed DSARs.
- □ You maintain records of past requests in a secure, organized location.

You've just identified your organization's DSAR readiness. But the journey from readiness to full-scale compliance requires the right tools. If your team is facing challenges with manual processes, limited visibility, or unorganized data, our platform is designed to fill those gaps.

Ready to Take the Next Step?

Don't just be ready, be fully prepared.
See how GAT Labs can automate your DSAR process and help you meet your compliance goals.

LEARN HOW IT WORKS