AutoPrivacy – DSAR Response Playbook (Solo-Founder Edition)

Why this matters

Data-Subject Access Requests (DSARs) let any user ask what personal data you hold, demand corrections, or request deletion. Regulators can fine up to **€20 M or 4 %** of global turnover for late or incomplete responses. This playbook shows a lean, ten-step process you can run—then automate with **AutoPrivacy**.

Key statutory deadlines

Regulation	Response window	Possible fines
GDPR (EU)	30 days (+60 with notice)	€20 M or 4 % of revenue
CCPA / CPRA (US-CA)	45 days (+45)	up to $7,500 per user
LGPD (Brazil)	15 days	2 % of revenue (BRL 50 M cap)

Step-by-Step Checklist

1. **Capture the request** — log date, channel, requester email; acknowledge within 24 h.
2. **Verify identity** — request two proofs (e.g., last invoice ID + account-email confirmation).
3. **Classify request type** — Access · Deletion · Portability · Rectification · Objection.
4. **Freeze retention jobs** — pause deletion/rotation tasks that might erase evidence.

5. **Locate data sources** — GitHub, Stripe, AWS logs, Google Workspace, HubSpot, support tickets.
6. **Extract user data** — run exports/API pulls filtered by user ID or email.
7. **Redact third-party info** — strip indirect identifiers belonging to other data subjects.
8. **Compile evidence pack** — PDF summary + CSV mapping (field → source → GDPR article).
9. **Deliver securely** — encrypted link, password separately, log delivery timestamp.
10. **Close & document** — update DSAR register, resume retention jobs, schedule deletion.

Automation Flow — how AutoPrivacy handles steps 5 - 8

Phase	***What happens***	***Outcome***
Data export	*The CLI uses read-only OAuth tokens to pull user-specific records from GitHub, Stripe, Google Workspace, etc.*	*You have a single, timestamped JSON bundle containing every system's raw data for the requester.*
Local PII scrubbing	*Before anything leaves your machine, the CLI removes indirect identifiers (IP addresses, third-party names, contact notes) and masks sensitive fields.*	*Only the requester's personal data remains; privacy for bystanders is preserved.*
Classification with GPT-4o	*The scrubbed data is passed to GPT-4o (from your machine) to tag each field with the relevant GDPR article (e.g., "Art. 15 – right of access").*	*A structured YAML file that maps field → source → legal basis—the backbone of your evidence packet.*

Evidence pack generation	*The CLI converts the YAML into a branded PDF summary plus a CSV mapping table, then encrypts the bundle and produces a shareable link.*	*A complete, auditor-ready response you can send immediately to the requester.*

Cycle time: *< 10 minutes end-to-end, vs. ~6 hours of manual work.*

ROI snapshot

Five DSARs / year → **save ≈ $6,400** compared with manual processing.
(Engineer time @ $80/h × 6 h/request)

Resources & next steps

- DSAR Register (Google Sheet)
- Email-acknowledgement boilerplate (GDoc)
- CLI quick-start script (GitHub)

Book a 15-min automation demo → https://autoprivacy.dev/demo

Questions? **hello@autoprivacy.dev**

AutoPrivacy