Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

PRIVACY ADVISORY SERVICE — OPERATIONAL PROCEDURE

DSAR Response Procedure

Step-by-Step Guide · Deadlines · Log Template

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

For implementation support, contact Axiom Sovereign. This document is for educational purposes.

Data Subject Access Request (DSAR) Response Procedure

About This Document

A Data Subject Access Request (DSAR) is a formal request from an individual to exercise their privacy rights under GDPR, CPRA, or other applicable privacy regulations. This document provides a step-by-step procedure for receiving, validating, and responding to DSARs within the legally required timeframes. Missing a DSAR deadline — even by one day — is itself a regulatory violation.

Response Deadlines by Regulation

GDPR (EU/UK): 30 calendar days from receipt. Extendable by 2 months for complex/numerous requests — but must notify the individual within the first 30 days that an extension is being taken.

CPRA (California): 45 calendar days from receipt. Extendable by an additional 45 days with notice to the individual within the first 45 days.

VCDPA (Virginia), CPA (Colorado), and most other state laws: 45 calendar days. Extension provisions vary by state — verify for your specific jurisdiction.

HIPAA (Patient Access Requests): 30 calendar days from receipt. One 30-day extension permitted with written notice.

STEP-BY-STEP DSAR RESPONSE PROCEDURE

STEP 1: RECEIVE AND LOG THE REQUEST (DAY 0)

The clock starts the moment you receive a DSAR — by email, mail, phone, or in person. Do not delay logging because you are uncertain whether the request is valid.

- Create a DSAR log entry immediately upon receipt (see DSAR Log template at end of this document)

- Record: date received, channel (email/mail/phone/in-person), requester name and contact information, description of rights being requested (access, deletion, correction, portability, opt-out)
- Assign a DSAR reference number
- Assign a responsible handler
- Calculate the response deadline based on applicable regulation and record it in the log
- Send an acknowledgment to the requester within 3 business days confirming receipt and estimated response date

STEP 2: VERIFY THE REQUESTER'S IDENTITY (DAYS 1–5)

You must confirm the requester is who they claim to be before disclosing any personal data. However, identity verification must be proportionate — do not request excessive documentation.

- For existing clients/patients: verify identity using information already on file (account number, date of birth, last transaction, previously provided contact details)
- For new or unverified requesters: request one form of government-issued ID (redacted to show name and photo only) OR two forms of non-ID verification (e.g., email address on file + last 4 of SSN)
- Do NOT require notarized documents, original signatures, or excessive ID for simple access requests
- If you cannot verify identity: request additional information and pause the response clock — but document this clearly and do not use identity verification as a delaying tactic
- For authorized agents (attorney, family member): verify both the requester's identity and their authority to act (power of attorney, written authorization)

STEP 3: SCOPE THE REQUEST (DAYS 3–7)

Determine exactly what data is being requested and where it lives in your systems.

- Identify all systems that may contain data about the requester: CRM, ERP, email, file storage, backup systems, accounting software, third-party platforms
- Determine the scope of the request: all personal data? Specific data types? Data from a specific period?
- Check whether any exemptions apply: legal privilege (for law firms), trade secrets, third-party data, law enforcement or regulatory holds, or data required for legitimate business purposes
- If deletion is requested: identify data subject to legal retention requirements (tax records, audit workpapers, healthcare records) that cannot be deleted
- Document your scope determination with reasoning for any data excluded from response

STEP 4: COMPILE THE RESPONSE (DAYS 7–21)

Gather all in-scope personal data and prepare the response package.

- Export or compile all personal data within scope from identified systems
- Review for third-party data — redact or exclude data that would disclose other individuals' personal information

- Review for privileged or exempt data and document any exclusions with legal basis
- Format the response: provide data in a common, machine-readable format where portability is requested (CSV, JSON)
- Prepare a cover letter explaining: what data is provided, the format, any exemptions applied and their legal basis, how to appeal or complain to the supervisory authority (required under GDPR/CPRA)

STEP 5: REVIEW AND APPROVE RESPONSE (DAYS 21–28)

Before sending, review the response for accuracy, completeness, and compliance.

- Legal or compliance review of any data excluded under an exemption claim
- Verify all in-scope data is included — search again if there is any uncertainty
- Confirm the response letter includes all required elements (identity of data controller, how to file a complaint with the supervisory authority, right to seek judicial remedy)
- Obtain approval from responsible officer or legal counsel for high-risk or complex DSARs

STEP 6: SEND RESPONSE AND CLOSE LOG (BY DEADLINE)

Deliver the response within the applicable deadline and update your records.

- Send response via a secure channel appropriate to the sensitivity of the data (encrypted email, secure portal, certified mail)
- Record the date of delivery in the DSAR log
- If the deadline cannot be met: notify the requester before the deadline, explain the reason for extension, and provide the revised response date
- Retain the DSAR response package (request, verification, response, cover letter) for 3 years minimum
- Update your DSAR log status to "Closed" and note any lessons learned for program improvement

DSAR LOG TEMPLATE

Field	Entry
DSAR Reference Number	
Date Received	
Channel (email / mail / phone / in-person)	
Requester Name	
Requester Contact Information	
Rights Requested (access / deletion / correction / portability / opt-out)	
Applicable Regulation (GDPR / CPRA / VCDPA / HIPAA / other)	
Response Deadline	
Extension Taken? If yes, date requester notified	
Assigned Handler	
Identity Verified? Date and method	
Systems Searched	
Data Excluded and Legal Basis	
Date Response Sent	
Outcome / Notes	
Status (Open / Closed)	

Ready to Get Started?

Schedule your complimentary 30-minute discovery call: calendly.com/cmissimore-6zkc/30min · info@axiomsovereign.com · axiomsovereign.com