Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

PRIVACY ADVISORY SERVICE — COMPLIANCE TOOL

Data Mapping Template & Record of Processing Activities

Client Data · Employee Data · Vendor Flows · Retention Schedule

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 Mapping Template & Record of Processing Activities

About This Document

A data map — also called a Record of Processing Activities (ROPA) under GDPR — is a documented inventory of all personal data your organization collects, processes, and stores. It is the foundational privacy compliance document. Without a data map, you cannot: respond accurately to DSARs, demonstrate GDPR Article 30 compliance, conduct HIPAA risk analysis, respond to regulatory inquiries, or implement data minimization and retention programs.

Who Needs This

GDPR Article 30 (Required): Organizations with 250+ employees, or any size organization that processes personal data "not occasionally" or processes special categories of data (health, biometric, etc.), must maintain a ROPA. Most professional services firms fall into this requirement.

CPRA and most U.S. state privacy laws: Require organizations to be able to respond to consumer data requests, which is impossible without knowing what data you hold and where.

HIPAA Risk Analysis: Requires identifying all ePHI — which requires knowing all systems that process, store, or transmit patient data.

Cyber insurance applications: Carriers ask what types of data you hold. Accurate answers require a current data inventory.

How to Complete This Data Map

Step 1 — Identify data owners: For each business function (HR, Finance, Client Services, Operations), identify the person responsible for the data used in that function. They complete the relevant rows.

Step 2 — Complete one row per data stream: A "data stream" is a specific type of personal data collected for a specific purpose. Client tax data collected for tax preparation is one row. Employee payroll data is another.

Step 3 — Be specific about systems: Name the actual software, not the category. "Accounting software" is not useful. "QuickBooks Online, company account, cory@axiomsovereign.com" is.

Step 4 — Review annually: Data maps become stale when you adopt new software, add services, or change vendors. Review and update at minimum annually and when material changes occur.

SECTION 1: CLIENT / PATIENT DATA

Complete one row for each distinct type of client or patient data your organization collects.

Data Type	Specific Data Elements	Collection Purpose	Legal Basis (GDPR)	System / Location	Third Parties With Access	Retention Period	Security Controls
Client Contact Data	Name, address, phone, email, company	Client relationship management	Contract / Legitimate Interest	[CRM name]	[List vendors]	[X] years after engagement ends	Encryption, access control
Client Financial Data	Account numbers, tax IDs, income, assets	Tax preparation / financial advisory	Contract	[Software name]	IRS, state agencies per service	7 years (IRS guidance)	Encryption, MFA, audit log
Client Legal Matter Data	Matter details, communications, documents	Legal service delivery	Contract / Legal Obligation	[DMS name]	Courts, opposing counsel per matter	Per applicable bar rules	Access control, privilege protection
Patient Health Information (PHI)	Demographics, diagnosis, treatment, billing	Healthcare service delivery	Contract (HIPAA: Treatment)	[EHR name]	Per BAA — [list]	HIPAA minimum: 6 years	Encryption, MFA, audit log, BAA
[Add rows as needed]							

SECTION 2: EMPLOYEE AND HR DATA

Data Type	Specific Elements	Purpose	Legal Basis	System	Retention
Employee Personal Data	Name, SSN, address, DOB, emergency contact	Employment / Payroll / Benefits	Contract / Legal Obligation	[HRIS / Payroll system]	7 years post-termination (tax)
Payroll and Benefits	Salary, bank account, benefits elections, W-2	Compensation and benefits administration	Contract / Legal Obligation	[Payroll software]	7 years (IRS)
Performance and Disciplinary	Reviews, PIPs, disciplinary actions	Employment management	Legitimate Interest	[HR system / Files]	Duration of employment + 7 years
Hiring and Recruitment	Resumes, interview notes, background checks	Hiring	Consent / Pre-contract	[ATS / Email / Files]	2 years (EEOC guidance)
[Add rows]					

SECTION 3: VENDOR AND THIRD-PARTY DATA FLOWS

Document every vendor that receives personal data from your organization.

Vendor Name	Data Shared	Purpose	Contract Type (DPA / BAA / None)	Vendor Country	Transfer Mechanism (if EU data)	Annual Review Date
[Cloud storage vendor]	Client documents, PHI (if applicable)	Document storage	DPA / BAA	USA	SCCs if EU data	[Date]
[Payroll processor]	Employee PII, SSNs, bank accounts	Payroll processing	DPA	USA	N/A	[Date]
[AI vendor — e.g., Microsoft Copilot]	Inputs to AI — specify data types	AI-assisted work	DPA / BAA (if PHI)	USA	SCCs if EU data	[Date]
[Add rows as needed]						

SECTION 4: DATA RETENTION SCHEDULE

Data Category	Retention Period	Legal Basis for Retention	Deletion Method
Federal tax records (returns, workpapers)	7 years from filing date	IRS Publication 583 / Statute of limitations	Secure deletion from all systems
HIPAA medical records (adults)	6 years from creation or last use	45 CFR §164.530(j)	NIST 800-88 compliant media sanitization
HIPAA medical records (minors)	Age of majority + 3 years or 6 years from creation, whichever is longer	45 CFR §164.530(j) + state law	NIST 800-88 compliant
Legal matter files	Per applicable state bar rules (typically 5–7 years post-matter)	ABA Model Rule 1.15	Secure deletion with privilege review
Employee records (post-termination)	7 years	EEOC / IRS / ERISA requirements	Secure deletion
Email (general business)	[X] years per Firm policy	Business records retention policy	Email archival purge

Ready to Get Started?

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