

Data Management Plan

A practical plan for what data you hold, where it lives, who can touch it, and when it gets deleted - the operational backbone auditors and enterprise buyers ask for.

BEST FOR
REGULATED OR SENSITIVE DATA

TIME TO COMPLETE
45-60 MINUTES

VERSION
JULY 2026

How to use this

Fill the inventory (Section 1) first - everything else references it. Keep this plan version-controlled next to your code or in your data room; it's the document that turns security claims into something you can actually show.

1 Data inventory & flow mapping

Every meaningful dataset you hold. If it isn't listed, it isn't governed.

#	Dataset	Category	Sensitivity	Source / how collected	System & region
1	e.g. user profiles	personal	medium	sign-up	Postgres / EU
2					
3					
4					
5					

Suggested sensitivity: public / internal / confidential / restricted. Mark personal, special-category, customer-confidential, secrets, and regulated data explicitly.

2 Storage, retention & deletion

One row per dataset above. Retention with no deletion trigger is just hoarding with extra steps.

Dataset	Encryption (rest / transit)	Retention period	Deletion trigger	Deletion method & owner
user profiles	AES-256 / TLS 1.2+	36 mo after last login	account closed	hard delete / Eng

Deletion evidence

How you prove deletion/anonymisation happened, including backups and subprocessors

Legal hold / investigation exception

Who can pause deletion, on what basis, and where it is recorded

3 Access control & role definitions

Least privilege in writing. Who can reach what, why, and how often it's reviewed.

Role	Systems / datasets	Access level	Justification	Review
Support	CRM (read)	read	handle tickets	quarterly

Quick checks

- MFA enforced on every system holding personal data
- Admin/production access is named, not shared
- Joiner / mover / leaver process revokes access promptly
- Access reviews leave evidence: date, reviewer, removals, exceptions

4 Third-party processors

Anyone who processes your data on your behalf. Each one needs a data processing agreement.

Processor	Purpose	Data shared	Region / transfer	DPA?	Reviewed
e.g. Stripe	payments	billing	US / SCCs	Y	2026-01

Subprocessors and transfer safeguards

Where subprocessors are listed, how changes are reviewed, SCCs / adequacy / transfer impact notes

5 Resilience & ownership

Backup schedule, location & last restore test

Overall data owner & next plan review date

Incident hook

Who is alerted when data is lost, exposed, corrupted, or retained beyond policy?

Need a practical compliance review?

This template gets you started. If you'd like an engineer who does compliance to pressure-test your answers - or turn them into working controls, documentation, and audit-ready evidence - book a free 30-minute discovery call.

[Book a free discovery call](#)

or visit rdelune.dev

This template is provided by rdelune LLC for general informational purposes only and does not constitute legal, regulatory, or professional advice, nor create a consultant-client relationship. Regulatory obligations depend on your specific facts and jurisdiction. Validate your completed document against the applicable law (e.g. the EU GDPR, the ePrivacy Directive, and the EU AI Act) and, where appropriate, with a qualified professional. © 2026 rdelune LLC. You may use and adapt this template freely within your organisation; please retain this attribution.