PERPETUAL SQUARED

Enterprise-grade cloud architecture, DevSecOps, and digital transformation consulting
perpetualsquared.com

Book a free 30-min strategy call
calendar.app.google/5Gkf1TgDBE3nRz9b6

GDPR-Ready Database Checklist

For backend engineers building privacy-compliant systems from day one.

1 Data Encryption · Art. 5(1)(f), Art. 32

- [ ] **Enable column-level encryption for PII fields** — Art. 5(1)(f) / Art. 32
  Encrypt name, email, DOB, address individually — not just full-disk. Enforce decryption in the query layer.
- [ ] **Use AES-256 for data at rest** — Art. 32
  Apply to all database volumes, backups, and snapshots. Verify encryption is enabled on managed DB services.
- [ ] **Enforce TLS 1.2+ for data in transit** — Art. 32
  All client-to-DB and service-to-DB connections. Reject unencrypted connections at the network level.
- [ ] **Rotate encryption keys on a defined schedule** — Art. 32
  Document key rotation policy. Use a secrets manager (AWS KMS, GCP KMS, HashiCorp Vault).

2 Right to Erasure (Right to be Forgotten) · Art. 17

- [ ] **Implement pseudonymisation over hard deletes** — Art. 17
  Replace PII with a token/UUID. Relationships and foreign keys stay intact. Audit trail preserved.
- [ ] **Map all PII foreign key dependencies before schema design** — Art. 17
  Identify every table referencing user_id. A deletion strategy must exist for all of them.
- [ ] **Create an erasure request workflow with SLA** — Art. 17
  GDPR requires erasure 'without undue delay' — typically within 30 days. Build this into your backlog.
- [ ] **Verify erasure extends to backups and archives** — Art. 17
  Hard deletes from live DB don't remove data from snapshots. Define a backup invalidation policy.

3 Data Residency & Storage Limitation · Art. 5(1)(e), Art. 44

- [ ] **Add a data_region column to tenant/user schema** — Art. 44
  Encode residency at schema level. Your infrastructure team should not be making compliance decisions.
- [ ] **Enforce residency constraints at the ORM layer** — Art. 44
  Queries for EU users must route only to EU regions. Test this with cross-region query interception.

- [ ] **Define and enforce data retention periods per data type** — Art. 5(1)(e)
  Don't store data longer than needed. Build automated TTL jobs or archival pipelines.
- [ ] **Document cross-border data transfer mechanisms** — Art. 46
  Standard Contractual Clauses (SCCs) or adequacy decisions required for transfers outside EEA.

4 Audit Logging · Art. 5(2), Art. 30, Art. 33

- [ ] **Create append-only audit tables in your database** — Art. 30
  Columns: user_id, action, resource_type, resource_id, timestamp, ip_address. Not in app logs.
- [ ] **Log all PII read, write, and delete operations** — Art. 33
  You must be able to answer: who accessed what data, and when. This is required for breach response.
- [ ] **Protect audit logs from modification or deletion** — Art. 5(2)
  Immutable storage. Separate access controls from production DB. Consider write-once S3 / Cloud Storage.
- [ ] **Test audit trail completeness before go-live** — Art. 33
  Simulate a breach scenario. Can you answer all Article 33 notification requirements from your logs?

5 Data Minimisation & Schema Hygiene · Art. 5(1)(c)

- [ ] **Add schema review to your PR checklist** — Art. 5(1)(c)
  For every new column: 'Is this PII? Do we need it? Could we store less?' Make this culture, not policy.
- [ ] **Replace exact values with derived flags where possible** — Art. 5(1)(c)
  date_of_birth → is_over_18. full_address → country_code. Store what you need, not what's available.
- [ ] **Audit existing schema for unnecessary PII columns** — Art. 30
  Run a PII discovery scan on your current schema. Document what you have and why you have it.
- [ ] **Document lawful basis for each PII field stored** — Art. 6
  Consent, contract, legitimate interest — each field needs a basis. This is your ROPA (Record of Processing).

Breach Response Reminder

Art. 33 — 72 hours from *awareness* to notify your supervisory authority. Not from your post-mortem. From the moment someone in your org knew.
Art. 34 — If risk to individuals is high, notify affected users directly. No fixed window — fast.

To notify properly you need:
- Nature of breach
- Categories and number of individuals
- Likely consequences
- Measures taken