RESOURCE

GDPR Starter Pack for Startups

What you actually need, in what order, without overbuilding

Does GDPR apply to my startup?

GDPR applies if you offer goods or services to individuals in the EU or monitor their behavior, regardless of where your company is based.

Phase 1: The basics (do this now)

- Privacy policy describing what you actually collect and why
- Cookie consent: opt-in before non-essential cookies for EU visitors
- Vendor DPAs with key processors, where applicable
- Understand what personal data you collect, where it goes, and your legal basis

Phase 2: Before first enterprise deal or funding round

- RoPA, DSAR process, breach response plan, DPA template
- DPO appointment if legally required or commercially expected

Phase 3: Scaling

- DPIAs, vendor risk management, employee training, AI governance, multi-jurisdictional compliance

Common mistakes

- Copying a competitor's privacy policy (it will not describe your practices)
- Assuming GDPR does not apply because you are outside the EU
- Appointing your CTO as DPO (often creates conflict of interest risk under GDPR)
- Thinking Vanta/Drata replaces a DPO (security tools, not DPO services)

Timeline and cost

Phase 1 takes days. Phase 2 takes 4 to 6 weeks with an outsourced DPO. An outsourced DPO for a startup commonly starts from EUR 500 to 2,000/month depending on scope.