

GDPR readiness checklist

The European Union law on handling personal data. Applies to anyone serving people in the EU.

What GDPR asks

- ☐ Lawful basis and principles: Have a valid reason to use data, and use it fairly and only as needed.
- ☐ Individual rights: Let people see, correct, delete and move their data.
- ☐ Accountability: Keep records, assess high-risk uses, appoint a DPO where needed.
- ☐ Security: Protect data with suitable technical and organisational measures.
- ☐ Breach response: Report serious breaches to the regulator within 72 hours.
- ☐ International transfers: Use approved safeguards when data leaves the EU.

Getting started

- ☐ Map your data: List what personal data you hold, where, and why.
 - ☐ Fix the basics: Privacy notices, consent, retention rules.
 - ☐ Cover your vendors: Data processing agreements and transfer checks.
 - ☐ Set up rights and breach handling: Clear owners and timelines.
 - ☐ Keep records and review: Update as systems and vendors change.
-

Official source

[eur-lex.europa.eu](https://eur-lex.europa.eu/eli/reg/2016/679/oj) (Regulation 2016/679) - <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Want a scored report by email? Run the free assessment at
<https://www.optimuscyberx.ai/frameworks/gdpr/assessment/>