

GDPR

Cheat sheet for the EU General Data Protection Regulation

The principles (Art. 5)

- Lawful, fair and transparent. Collected for a specific purpose. Only what you need (data minimisation).
- Accurate. Kept no longer than necessary. Kept secure (integrity and confidentiality).
- You must be able to show you comply (accountability).

Legal bases (Art. 6)

- Consent, contract, legal obligation, vital interests, public task, or legitimate interests. Pick and document one before you process.

People's rights

- Be informed, access, rectify, erase, restrict, port their data, object, and not be subject to solely automated decisions with significant effects.
- You normally have one month to respond to a request.

Breaches (Art. 33-34)

- Tell your supervisory authority within 72 hours of becoming aware, unless the breach is unlikely to put people at risk.
- Tell the affected people without undue delay if the risk is high.
- Document every breach, even ones you do not report.

Penalties (Art. 83)

- Up to EUR 20 million or 4% of worldwide annual turnover for the most serious violations; up to EUR 10 million or 2% for others.

First five actions

- 1. Map the personal data you hold. 2. Record the legal basis for each use. 3. Write or update your privacy notice. 4. Sign data processing agreements with suppliers. 5. Prepare a breach and a rights-request procedure.