GDPR Audit Checklist

Scope, records, rights, vendors, security and follow-up

Use this checklist to prepare a GDPR compliance audit. Each item is a question to check internally. A **no** or **not sure** marks a point to secure before an audit or a client request.

Framework	When it applies to you
Moroccan law 09-08 / CNDP	All processing carried out in Morocco: clients, prospects, staff, website.
EU GDPR	Once you process data of people located in the EU, or target the European market.

1 Scope and governance

- ☐ The entities, locations, products and systems in scope are identified.
- ☐ Business, IT, security, HR and leadership owners are identified.
- ☐ Previous audits, incidents, DPIAs and action plans have been gathered.
- ☐ Materiality criteria and a scoring method are defined.

2 Records and legal bases

- ☐ Actual processing activities have been compared to the record of processing.
- ☐ Purposes are written specifically, not generically.
- ☐ A legal basis is documented for each purpose.
- ☐ Retention periods are justified.
- ☐ Categories of people and data are complete.

3 Transparency and rights

- [ ] Privacy notices for clients, staff, candidates and users are up to date.
- [ ] A channel for receiving rights requests is identified.
- [ ] Identity verification is proportionate to the request.
- [ ] Deadlines, exceptions and responses are logged.
- [ ] A request has been tested end to end.

4 Vendors and transfers

- [ ] The list of processors and their roles is kept up to date.
- [ ] Article 28 contracts are available.
- [ ] Sub-processors and their locations are known.
- [ ] Access from outside Morocco/the EEA is identified.
- [ ] Standard contractual clauses and supplementary measures are documented where needed.

5 Security and incidents

- [ ] Access, permissions and leavers are controlled.
- [ ] Backups, encryption and logging are documented.
- [ ] A breach register is available.
- [ ] Escalation and risk analysis have been tested.
- [ ] CNDP notification and communication are prepared.

6 Reporting and follow-up

- [ ] Findings are linked to evidence.
- [ ] Risks and priorities are explained clearly.
- [ ] Owners and deadlines are assigned.
- [ ] Closure evidence is defined for each action.
- [ ] The limits and exclusions of the work are stated.

Next step with RCM

RCM can run this audit with you, prioritize the gaps and prepare what's expected: records, policies, DPAs and CNDP filings.

Book a call: calendly.com/rgpdconseilmaroc-reunion/30min
ElMahdi El Khalouki | +212 6 88 89 06 02

This checklist is general guidance and does not replace an audit or legal advice for your specific situation.