recordia

GDPR Compliance Checklist

Record of explicit consent:

- ☐ Consent is **freely given, specific, informed and unambiguous**.
- ☐ Consent requests are "clearly distinguishable from other matters" and are presented in **"clear and plain language"**.
- ☐ Interested individuals **may withdraw previously given consent whenever they wish to do so**, and their decision must be respected.
- ☐ **Children under the age of 13** can only give consent with parental permission.
- ☐ You retain the **documentary proof of consent**.
- ☐ When **you update your privacy policy**, you inform existing customers.

Legal basis & transparency:

- ☐ You **audit information to determine what information you process** and who has access to it.
- ☐ **You have a legal justification for your data processing activities**. Processing is only valid when it is necessary to:
    - Comply with a contract.
    - Satisfy legal requirements.
    - Protect the interests of one or more participants.
    - For security or the data is in the public interest.
    - Responds to the legitimate interests of the registrar, provided that those interests are not overridden by the interests of data subjects requiring protection of personal data.
- ☐ You provide **clear information about data processing and legal justification** in your privacy policy.

recordia

Data security:

- ☐ **Personal data is stored securely, and appropriate security controls are implemented** to prevent any unauthorized persons from accessing stored personal data.
- ☐ **Personal data is encrypted, pseudonymized or anonymized** whenever possible.
- ☐ You conduct a **data protection impact assessment** whenever you plan to use individuals' data in a way that is likely to result in a high risk to their rights and freedoms.
- ☐ You have a **formal process implemented to notify the authorities (within 72 hours) and your data subjects** in the event of a data breach.

Responsibility & management:

- ☐ **Your company has appointed a Data Protection Officer (DPO) if it is necessary**, when processing is carried out by a public authority, the processing is the core business of a large-scale organization or special category data is processed.
- ☐ **You train staff to be aware of data protection**.
- ☐ **You sign a data processing agreement between your organization and any third-party** processing personal data on your behalf.
- ☐ **If your organization is outside the EU, you appoint a representative within one of the EU members' states**.

Privacy rights:

- ☐ It's easy for your customers to **request access to their personal information**.
- ☐ It is easy for your customers **to update their own personal information** to keep it accurate.
- ☐ The **deletion of data that is no longer needed is automated**.
- ☐ It's easy for your customers to **request to stop processing their data**.
- ☐ It's easy for your customers to **request to have their personal data deleted**.
- ☐ It is easy for your customers to **request to have their data transferred to them or to a third party**.
- ☐ It is easy for your customers to **object to you processing their data**.