



GDPR Compliance Checklist

1. Data Awareness & Mapping

- I know what personal data my business collects and where it's stored.
- I know who has access to personal data.
- I've documented all data processing activities.

2. Legal Basis & Consent

- I have identified a lawful basis for processing each type of data.
- I obtain clear consent where required and keep records of it.
- I provide an easy way for people to withdraw consent.

3. Data Security

- I use passwords, encryption, or MFA to protect sensitive data.
- I have procedures for managing data breaches.
- Staff are trained on data protection and safe handling of information.

4. Privacy Notices

- I have an up-to-date privacy policy written in plain English.
- It tells people how and why I use their data.
- It includes contact details and data rights information.

5. Data Rights & Requests

- I have a process for handling Subject Access Requests.
- I can correct or delete personal data when requested.
- I respond to requests within one month.

6. Data Retention & Deletion

- I only keep data as long as necessary.
- I have a regular deletion or anonymisation schedule.

© Novo Data Services