GDPR Compliance Checklist

**Obtaining consent**

People must proactively give you consent to store their data.

| **To do**  | **Done** |
| --- | --- |
| Ensure consent request is unbundled (not just hidden in T&C’s) |  |
| Ensure consent is actively given (not a pre-checked box) |  |
| Make it clear who consent is given to (not just ‘third parties’) |  |
| Document it (keep a record of the consent given) |  |
| Make it easy to withdraw |  |
| Publish a privacy policy that includes the use of cookies |  |

**Supporter information**

How to handle supporter data that is given to you.

| **To do**  | **Done** |
| --- | --- |
| Have an unchecked, opt-in button on your donation form |  |
| Keep a record of the consent that has been given in your database |  |
| Keep a central record of communication preferences |  |
| Enable people to easily unsubscribe or change their preferences |  |

**General compliance checks**

| **To do**  | **Done** |
| --- | --- |
| Specify who’s responsible for data protection in your organisation |  |
| Train your staff keeping data secure and up to date |  |
| Register with the ICO |  |
| Have a policy for dealing with people’s requests to access their data |  |
| Make sure you have legitimate reasons to collect data |  |
| Have a policy on how you properly delete out-of-date information |  |
| Publish the steps you take to ensure data security |  |
| If you use third party tools, make sure they are compliant |  |