

General Data Protection Regulation

Top Tips for GDPR Compliance

- 1 Nominate someone at your organisation to be responsible for data protection compliance.
- 2 Understand what personal data you collect and why, who you share it with, how long you need to keep it for and how you protect it. To do this you can carry out an audit to see how your existing procedures are in line with GDPR requirements.
- 3 Make sure you can legally justify having each item of personal data. Consent is unlikely to be the most appropriate option going forward due to the increased conditions to obtain valid consent.
- 4 Amend your privacy notices and privacy policies to include all of the new things that must be included. Remember, also, your notices and policies must be concise and intelligible. Provide the new version to all data subjects. We have created template membership forms and privacy notices to help you.
- 5 Encrypt personal data in any electronic devices and when sending it to anyone electronically e.g. password protecting any spreadsheets that contain personal information.
- 6 Make sure that sensitive documents are filed away immediately after printing.
- 7 As part of minimising the data you hold, avoid duplication of sensitive information and documents.
- 8 Update data often to keep it current and avoid errors.
- 9 Make sure you can satisfy requests for access within a month and can comply with other rights of individuals.
- 10 Make sure you maintain records to demonstrate that you comply with the rules.
- 11 Make sure you train your staff and volunteers to follow the new law and your processes.
- 12 Get help from the Information Commissioner's Office (www.ico.org.uk)