

General Data Protection Regulation

TOP 10 TIPS TO CONSIDER

1 Have you created awareness?

- Staff should be made aware that the law is changing to GDPR.
- They need to appreciate the impact that this will have and how the company will need to plan to meet those commitments and evidence of compliance.

1

2 Have you nominated someone to be responsible?

You should nominate someone to be responsible for data protection compliance and assess where the role will sit within your organisation's structure and governance arrangements.

2

3 Do you know what information you hold?

- You need to document what personal data you hold, where it came from, consent received and who you share it with.
- You may need to organise an information audit to do this.

3

4 Are your privacy notices sufficient or do you have any?

You need to review your current privacy notices and put a plan in place for making any necessary changes in time for the GDPR implementation deadline.

4

5 Can you facilitate the rights of individuals?

- Check your procedures to ensure they cover all the rights individuals have, including how you would document your processing activities.
- Clearly document all the data you hold.
- Provide data electronically & in a commonly used format (portability).

5

6 Can you handle subject access requests?

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6

7 How do you handle or obtain consent?

- You should review how you seek, record and manage consent and whether you need to make any changes.
- Refresh existing consents now if they don't meet the GDPR standard.

7

8 What do you do if there is a data breach?

You need to ensure you have the right procedures in place to detect, report and investigate a personal data breach.

8

9 How do you implement Privacy by Design and perform Data Privacy Impact Assessments?

You need to familiarise yourself with the various codes of practice on Privacy Impact Assessments and work out how and when to implement them in your organisation.

9

10 Is your organisation an international organisation?

If your organisation operates in more than one EU member state (i.e. you carry out cross border processing), you should determine your lead data protection supervisory authority.

10