

Preparing for the General Data Protection

Regulation (GDPR) 12 steps to take now

1

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2

Information you hold

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

3

Communicating privacy information

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

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5

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

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7

Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8

Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10

Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11

Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12

International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

