Preparing for the General Data Protection Regulation (GDPR) with BGi.uk.com/cyber

12 steps to take now

1 Awareness

You should make sure that decision makers and ley 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 need to organise an information audit.

3 Communication 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 should 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 Lawful Basis for Processing Personal Data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 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.

8 Children

You should start thinking now about whether you need to put systems in place to verify people's ages and to obtain parental or guardian consent for any data processing activity.

9 Data Breaches

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

10 Data Protection by Design and Data Protection Assessments

You should familiarise yourself with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and asses where this will site within your organisation's structure and governance3 arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you with this.

Source ico.
The Information Commisioners Office.
ico.org.uk

Key to Making You More Resilient