GDPR: THE 12 STEPS YOU MUST TAKE NOW

1. Awareness in North America

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR for doing EU business. 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.

3. Privacy Info Communication

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. 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 individuals' 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 place to prevent, detect, report and investigate a personal data breach.

10. Data Protection by Design, Data Protection Impact Assessments (DPIA)

You should familiarise yourself now 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 assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer

12. International Responsibilities

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. Article 29 Working Party guidelines will help you do this.

QA Consultants

https://qaconsultants.com/