Preparing for GDPR

12 steps to take now

For more information **call: 0800 198 7943**

PENINSULA

brighthr

Source: ICO - Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now

Get prepared for GDPR, 12 key steps

1. **Awareness**
Do the relevant people in your company know that the law is changing? Those who run businesses need to be aware of this and appreciate the impact the new regulations are likely to have.

2. **Information you hold**
What personal information do you currently hold, where did it come from and who do you share this with? By conducting an information audit you can start to fully understand your current information situation and be better prepared for the changes under GDPR.

3. **Consent**
Under GDPR organisations will need to get informed consent from the data subject in order to process their data. This will require a review in terms of how you seek, record and manage consent as well as refreshing existing consent if it doesn't meet the new standards.

4. **Individuals' rights**
Individuals will have increased rights in terms of access and erasure under GDPR. You should check your procedures to ensure you are covering these, including how you would delete personal data or provide data electronically if requested.

5. **Subject access requests**
How will you handle subject access request in the future? GDPR sets out new timescales and the information that will need to be provided, so it's important to have updated processes in place.

6. **Data breaches**
A data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Having a process to detect, report and investigate any data breach is essential, and those who do not follow procedures may face large fines.

7. **Communicating privacy information**
Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

8. **Children**
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. **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.

10. **Data Protection by Design and Data**
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 (DPO)**
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation. You should also consider whether you are required to formally designate a Data Protection Officer.

12. **International**
Does your organisation operate across the EU? If so you'll need to determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

PENINSULA

brighthr