GDPR Checklist

1 **Don't panic, whatever stage of GDPR preparedness you are at – stay calm and just keep going. GDPR is a journey not a destination**

2 **Awareness and education**

Ensure all key stakeholders understand what GDPR is and the implications for the business.

3 **Appoint a Data Protection Officer**

4 **Conduct a thorough data audit and document ALL the personal data you hold**

This means looking at any information you possess that identifies an individual across your business.

5 **Identify your lawful basis for processing**

There are six lawful bases for processing personal data under GDPR: Consent, Contractual, Legal Obligation, Vital Interests, Public Task and Legitimate Interests. It is important to note that there is no hierarchy - *all the legal bases have equal weighting.*

6 **Review your Privacy Policy and define any changes needed for GDPR**

GDPR states that a privacy statement should be transparent what data is collected and used, for what specific purposes, the existence and consequences of profiling, who is doing this processing, for what time periods and who will receive the data.

7 **Consent**

If you are using Consent as your legal basis for processing it must be:

- ☑ Unbundled
- ☑ Collected via active opt-in (pre-ticked opt-in boxes are invalid)
- ☑ Granular
- ☑ Named
- ☑ Easy to withdraw

8 **If you are using Legitimate Interest as your legal basis**

GDPR Recital 47: The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests and must carry out a three stage Legitimate Interest Assessment (LIA).

9 **Implement Data Protection by Design and by Default**

GDPR makes privacy by design an express legal requirement and requires that organisations need to consider privacy for every process and system.

10 **Review your process for data breaches and Subject Access Requests (SARs)**

GDPR creates new obligations regarding reporting of data breaches and processing of SARS – review all related policies and processes and amend accordingly.

REaD Group

readgroup.co.uk