GDPR Checklist

GDPR is undoubtedly a major challenge for most organisations. These questions are intended to help you assess how well your data security and usage controls compare to the GDPR requirements and help identify areas for improvement.

1. Does your organisation adhere to the 'privacy by design' principle? E.g. have you defined the legal basis for storing and using specific items of personal data?

2. Have you identified all your organisation's data and data sources? E.g. how confident are you that you know all the locations where your data resides?

3. Have you classified your organisation's data based on a sensitivity and confidentiality levels? E.g. do you have data classification policies and procedures in place?

7. Are you able to respond appropriately to Subject Access Requests (SAR)? E.g., can you provide all the information you hold on an individual promptly and accurately? Do you have processes in place to achieve the 'right to be forgotten'?

8. Are staff aware of your organisation's data protection requirements? E.g. what training programmes do you have in place?

9. Who is your organisation's designated point of contact for data protection? E.g. do they have a clear list of responsibilities?

4. Has your organisation obtained consent to hold and use individuals' data? E.g. can you check that consent has been obtained for each purpose e.g. through the use of engagement letters?

5. How is your organisation securing its data at rest and in transit? E.g. have you applied data encryption and anonymisation techniques where appropriate?

6. Do you have clear guidelines around data retention? E.g. have you defined data retention periods and data disposal policies and procedures?

10. How will your organisation ensure it is complying with the GDPR requirements? E.g. do you monitor compliance via internal and external reviews?

11. How does your organisation manage data breaches? E.g. do you have documented procedures to identify, report and investigate a personal data breach?