1. EDUCATE

Raise awareness across all aspects of your business involving staff from all relevant departments. GDPR will apply to all companies doing business in the EU, so make sure overseas colleagues are involved and up to speed.

2. STAY ACCOUNTABLE

Accountability is a key driver of GDPR. So start by documenting what personal data you hold and identify areas of risk. Make certain you understand where the data comes from and whom you share it with. Consider running an information audit.

3. MAKE SURE YOU'RE LEGAL

The GDPR Introduces the Six Privacy Principles as the pillars of the legislation:

Principle 1 is the key and states that PII must be processed Lawfully, Fairly and Transparently.
The lawfulness of the processing will be dependent on the business. Organisations require a legal basis to process personal data under the GDPR. There are six offers, six legal bases:

- Consent
- Contracts
- Legal compliance (with another law)
- Protecting the vital interests of a person
- Public interest
- Legitimate interest

4. GET THE RIGHT CONSENT

Consent plays a key role in the GDPR, which greatly strengthens existing rules. Under GDPR, consent has to be freely given, specific, informed and unambiguous and requires a positive action from the individual. If you process sensitive personal data, consent will have to be explicit.

5. PSEUDONYMISATION

GDPR introduces Pseudonymisation for the first time into EU law. Pseudonymisation is a process that data goes through to ensure it is no longer directly linked to an individual. Personal data that does not have any directly identifying details could also be pseudonymised at the point of collection. For example, a randomised cookie ID that allows a user to be recognised but not directly identified.

6. GET YOUR COMMUNICATIONS SORTED

Transparency is another core element of the GDPR, which requires different levels of detail depending on whether you obtain the data directly from the individual or not. In all cases, your notice has to be concise, easily accessible and written in clear and plain language. It will also have to include the legal basis you use and explain your legitimate interest in processing personal data (Principle 2 Article 5 Clause 1).

Look carefully at the privacy notices you currently use and analyse what needs changing: and not only documentation, but also all internet publications.

7. MAKE SURE YOU UNDERSTAND THE RIGHTS THAT GDPR AFFORDS INVIDUALS.

These are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision making, including profiling

Check your processes to ensure that you can adequately respond to any requests you might receive from individuals.

8. DATA CONTROLLERS AND DATA PROCESSORS

GDPR maintains the notions of ‘data controller’ and ‘data processor’ found in current data protection law. Data Controllers are organisations that use data. Data Processors act on behalf of the data controller. Under current rules only the controller is held liable for data protection compliance, but GDPR extends statutory obligations to data processors.

Given that, both controllers and processors will have obligations under GDPR, Think carefully about your precise role. Start working on contracts with partners and review those that are already in place to ensure they are in line with GDPR requirements.

9. DATA BREACHES

Put in place processes that allow you to detect, report and investigate a breach. Identify those types of data that may trigger the notification requirement.

10. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

Privacy Impact Assessments (PIA) and Data Protection Impact Assessments (DPIA) play a significant role in the new rules. Under GPDR it will be a legal requirement for you to run a PIA in high-risk situations.
Carrying out a PIA before implementation, can help you assess how to incorporate these two principles into any new products or services you want to bring to market. DPIA should be ingrained in project management or process improvement incorporating the DPIA process and Risk assessment methodologies in to BAU (Behavioural Analysis Unit) on any technology process improvement.

11. DATA PROTECTION OFFICERS

One of the criteria needed to decide whether you need to designate a Data Protection Officer (DPO) is where ‘the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale’. Public sector organisations are mandated to appoint a DPO. The roles and criteria for other business are dependent on the three specific criteria based on the nature of the data processed. Article 37 (DCP ref page 45)

If this applies to your company, then you must appoint someone with the responsibility for your own GDPR compliance. You will also have to think where in the business structure and governance, this person will fit in.

12. INTERNATIONAL IMPLICATIONS

If you operate in a number of European countries, you need to identify which Data Protection Authority will be your “lead authority”. (International data transfer in GDPR is quite detailed with Brexit this opens additional considerations: particularly when outsourced data by a British company to India about European subjects. The options would require some detailed planning and process mapping and may require a two or even three pronged approach.

You should also think about your options for transferring data to countries outside the EU. (In addition need to check the list of countries that the GDPR stipulate are compliant for data transfer. Common sense says you wouldn’t want to transfer data to certain countries in the world. This is similar to rules and process in UK on Intelligence transfer to some countries: or recent example where the US published sensitive material about Manchester bombings.)