ADEPT 4

IT AS A SERVICE

GDPR Action Plan

Don't over-complicate GDPR – make it simple and follow the Adept4 GDPR action plan

STEP 1

Perform a gap analysis and audit data

- Identify where data is on the information estate and how it is classified;
- Look at data handling processes and procedures and how data is stored in terms of the company IT infrastructure;
- Examine how sensitive data is segregated and/or anonymised to protect the identity of data subjects and to ensure there is no risk of re-identification.

STEP 2

Consider if you need consent

- Review existing customer consent processes and revise as necessary;
- Update website forms, data capture processes and terms and conditions;
- Look at how you obtain consent for under 18's and bear in mind that data held for under 13's must be supported by parental consent;
- Be aware that explicit consent is not a prerequisite – you can establish compliance through the demonstration of lawful processing.

STEP 3

Review contractual arrangements with suppliers/partners

- Understand whether partners and suppliers are compliant and whether they have the procedures in place to protect the data they share with you/you share with them and be prepared to renegotiate contracts on this basis to ensure compliance.

STEP 4

Assess how data is managed

- Examine the processes you have in place to allow content to be accessed, ported, redacted or deleted so that should you receive customer requests these they can be quickly actioned;
- Look at how data is managed in different locations such as on premise or in the cloud and whether data is sent abroad for processing;
- Look at data security measures and seek solutions that have privacy by design and ensure encryption of data both in transit and at rest.

STEP 5

Establish if you need a Data Protection Officer (DPO)

- Not all businesses will warrant the appointment of a DPO and those that do can assign responsibility to an existing member of staff provided there is no conflict of interest. Businesses who do handle large volumes of personal data will need to appoint a DPO (or outsource this capability) as stipulated under **Article 37** (find out here if your business requires a dedicated DPO).

Test your Incident Response capabilities

- Look at the data breach plan and test this to ensure that data is adequately protected and that you can notify the relevant authorities and/or customers within the necessary timefrae (without delay if the breach infringes rights or within 72 hours);
- Business continuity is vital to ensure the company can continue to operate, so look at other issues such as data back-up.

STEP 6

STEP 7

Determine if you can demonstrate accountability

- Ensure that the steps you have taken are documented and reviewed periodically to ensure that if the regulator does ask for evidence you can demonstrate due diligence.
- Explore whether you would be required to carry out Data Protection Impact Assessments (DPIAs) (generally these are only applicable to new technologies, where data is deemed to be at risk of exposure, or when processing high volumes of personal data).

For many SME organisations it's being able to prove due diligence that will be the most important aspect particularly given that a breach higher up in the supply chain may see the subsequent investigation include them. For example, a breach could see the cloud provider and associated suppliers deemed guilty by association requiring them to prove they had taken all the steps necessary and were lawfully processing data.

But determining whether you have taken sufficient steps to meet the new legislation presents the SME with a dilemma. They may not have the oversight, resource or time to delve into their data.

At Adept4 we assist with GDPR compliance by identifying data, assessing current data processing practices and outlining how this can be revised in line with the new requirements. Contact us today to find out more about how we can help you prepare for the GDPR. Or take our quick GDPR Readiness Assessment to establish where you need to focus resource on the road to compliance.