BULLET PROOF

10 STEPS TO GDPR COMPLIANCE

The journey towards General Data Protection Regulation (GDPR) compliance is not necessarily an easy one and many organisations are inadequate in their data protection obligations.

Failure to meet the requirements of the GDPR represents an increased risk of data breaches and the reputational damage and legal repercussions that inevitably follow. For those organisations in need of some guidance on achieving and maintaining compliance, we have compiled 10 steps to get you started.

1 DATA FLOW MAPPING

You need a record of where personal data enters your business, who accesses it, where it's stored, how it's stored and where it leaves the business.

2 RECORDS OF PROCESSING

You must document what personal data you are processing, the purposes, use, lifespan and security measures in place to protect it.

3 RISK FRAMEWORKS AND RISK ASSESSMENTS

You must assess the risk of data processing to the business and the data subject. A risk framework ensures new and existing risks can consistently be assessed.

4 LAWFUL BASIS FOR PROCESSING

When processing personal data, you must have documentation identifying a lawful basis to do so. If you do not have one, you cannot process personal data.

5 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

You are required to conduct a DPIA when processes and activities may present a high risk to the data subject to demonstrate threats have been considered and suitable controls implemented.

6 PRIVACY NOTICE

You must provide privacy notices (typically on your website) to data subjects to ensure you are transparent on how you collect, process, use, disclose and manage personal data.

7 THIRD-PARTY RELATIONSHIPS

Ensure you have suitable contracts in place with any third party that you share personal data with, clearly explaining the data protection obligations.

8 INTERNATIONAL TRANSFERS

In circumstances where you are transferring personal data outside of the EU you need to consider what additional safeguards are needed to protect this personal data.

9 POLICIES & PROCEDURES

You must be able to demonstrate how you are protecting the privacy of personal data with a robust set of policies and procedures. These will also ensure everyone in the business understands their data protection responsibilities.

10 APPOINTING A DATA PROTECTION OFFICER (DPO)

This is a mandatory requirement for some organisations, but the Information Commissioner's Office (ICO) recommends that all businesses appoint a DPO to be accountable for data protection. Outsourcing this to a reputable company on a retainer basis is often the most cost-effective way of managing this.

TAKE THE SMART APPROACH TO DATA PROTECTION

Your data protection obligations are an on-going process that requires continuous management. Get in touch with our team of certified DPOs and GDPR practitioners for help maintaining GDPR compliance and reducing the risk of data breaches.

BULLET PROOF

bulletproof.co.uk
01438 532 900
contact@bulletproof.co.uk