BULLET PROOF

HOW TO MAINTAIN GDPR COMPLIANCE

Businesses that hold personal data are 55% more likely to experience a breach or attack. With 46% of all UK businesses experiencing a cyber security breach or attack in the past 12 months, it is vital to ensure you have not only achieved GDPR compliance, but you are maintaining that same level of assurance.

46% UK BUSINESSES BREACHED IN 12 MONTHS

Many companies fall out of compliance by failing to reassess and amend their security processes as the business and the cyber security landscape change. Use our guide to identify the areas to evaluate and maintain your GDPR compliance.

TRAINING

This is an ongoing requirement for all new recruits joining the business but conducting annual GDPR refresher training for all staff will boost awareness. Sharing knowledge on security breaches and phishing attacks will also help your workforce understand and limit the risks.

RECORD AND ADDRESS DATA BREACHES AND DATA SUBJECT REQUESTS

If the ICO conducts an audit on your business, they will expect to see an up-to-date record of data breaches and data subject requests. Keep these updated with any new activity to avoid falling short of compliance.

REVIEW AND MAINTAIN RECORDS OF PROCESSING ACTIVITIES

These will change over time as you collect new data, adapt, or stop conducting certain processes. The person responsible for data protection in your business must be informed of any changes that could affect the validity of records.

REVIEW SECURITY MEASURES

A key element of the GDPR is ensuring there are suitable technical and organisational controls in place to protect personal data. Carrying out regular vulnerability scanning and penetration tests to assess technical controls is strongly advised, as is an annual GDPR audit to assess organisational controls.

CONDUCT DPIAS

You might need to conduct Data Protection Impact Assessments as you adopt new processes in the business. These also help increase awareness of privacy and data protection issues among staff members and help to ensure risks to the rights and freedoms of data subjects are addressed.

REGULAR RISK ASSESSMENT REVIEWS

You will need to be regularly analysing, assessing and mitigating risks within the business. Consideration of risk is fundamental in organisational accountability and you must be able to demonstrate how you carry out risk assessments and that risks are reviewed on a regular basis.

ENSURE DATA PROTECTION BY DESIGN IS BEING MAINTAINED

Data protection by design is about adopting an organisation-wide approach to privacy considerations. Building data protection as a key factor into projects early on ensures you comply with the GDPR's fundamental principles and requirements.

REVIEW AND MAINTAIN DATA FLOW MAPPING

Each department within your organisation will have different data processes. Departmental managers should be tasked with ensuring data flow maps are up to date and relevant to the interaction points they have.

DOCUMENTATION REVIEWS

Policies and procedures get out of date so you will need to review your documentation periodically. At least once a year address any changes, responsibilities and GDPR rulings which could impact your documents.

CONTRACT REVIEWS

Contracts with processors and other joint controllers should also be reviewed periodically to ensure they are up to date. Check whether anything has changed that might affect what is in the contract or your data processing obligations.

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 500 500
contact@bulletproof.co.uk