THE 7 STEPS TO ENSURING GDPR COMPLIANCE

The **General Data Protection Regulation** comes into force on 25th May 2018. The first substantial change to data regulation in the UK since the previous Data Protection Act was enacted in 1998, GDPR substantially tightens and toughens the requirements on businesses storing, sharing, sending and receiving the personal data of EU citizens.

Personal data is defined to be "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

Under GDPR, businesses are required not only to comply with requirements but to demonstrate their compliance. Firms must ensure that data protection is designed into their business processes, adhering to the principles of Privacy by Design and Privacy by Default (Article 25). Such measures may typically include data pseudonymisation or encryption (Recital 78).

Why is this important? The maximum fine for failing to comply is €20m.

1. Update privacy notices

You need to explain to clients via updated privacy notices why you are collecting their information, what you will be doing with it, how long you will keep it, who will have access to it, and where it will be stored. Ensure that clients actively confirm their acceptance (opt-outs will not suffice).

2. Identify personal data you hold

You should identify all personal data that you are holding, including where and how it is shared. Remove any personal data you do not require and ensure that all personal information is kept secure and only used for the purpose for which it was collected.

3. Use secure email

GDPR applies to external email and other communications as much as it does to internal processes. Sharing of personal data such as name, address, age etc. needs to be done securely. Use secure email to send or receive data from clients or other external contacts.

4. Prepare a plan for data breaches

You should have a plan for dealing with a data breach. This plan should detail what processes you have in place to detect a breach, stop the breach, prevent further breaches, and to communicate the breach to all affected individuals (and the regulator) within 72 hours.

5. Prepare to delete customer data

Clients have the right to demand that all their personal data be deleted (within certain parameters) and that proof of such deletion is provided to them. You should have processes in place to locate and delete customer data.

6. Prepare for data access requests

Customers have the right to know what personal data you hold on them and to request an electronic copy of their data at any time. You need to deliver the data securely and in a usable electronic format within 30 days.

7. Build a data protection culture

Make sure that all your employees are aware of the importance of complying with GDPR. Encourage them to think of personal data as a valuable commodity which needs to be protected at all times. Ideally, you should appoint a Data Protection Officer to be responsible for checking regulation, implementing and documenting processes, and ensuring adherence.

StayPrivate ensures safe and secure GDPR-compliant communication between businesses and external contacts.