THE 7 STEPS TO ENSURING GDPR COMPLIANCE

(AND HOW STAY PRIVATE HELPS)

The **General Data Protection Regulation** comes into force on 25th May 2018. GDPR reflects the increasing ubiquity of electronic data since the previous Data Protection Act was enacted in 1998, substantially tightening and toughening the requirements on companies 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.”

Companies are required not only to comply with but to demonstrate their compliance with GDPR. Businesses are also expected to implement measures to ensure that data protection is designed into the development of business processes for products and services, adhering to the principles of Privacy by Design and Privacy by Default (Article 25). Such measures may include data pseudonymisation or encryption (Recital 78).

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

1. Privacy Notices

You need to explain to clients via updated privacy notices why you are collecting data, 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. Implement a two-step confirmation process from your clients to confirm they have understood.

2. Identify Personal Data

You need to identify what personal data you hold, where and how it is shared. Remove any personal data you do not require and ensure that all personal data is kept secure and only used for the purpose for which it was gathered.

3. Implement Secure Communications

GDPR applies to external communications as much as it does to internal processes. Sharing of personal data such as name, address, age etc. needs to be done securely. If you send or receive data from clients or other external contacts via email, you must ensure communications are properly encrypted.

4. Plan for Data Breaches

You need a detailed plan documenting how you deal with a data breach. Make sure that you have processes in place to detect a breach, assess where the breach occurred, stop further breaches and communicate the breach to all customers affected with 72 hours.

5. Deleting 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 will need processes in place to locate and delete the data.

6. Delivering Data Access Requests

Customers also 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

Brief staff on the importance of complying with the GDPR. Encourage them to think of personal data as a valuable commodity which needs to be protected constantly. Appoint a Data Protection Officer to be responsible for checking the regulation, implementing procedures and ensuring adherence.

STAY PRIVATE is a simple tool for delivering GDPR-compliant secure communications (points 3 and 6 above).