GDPR COMPLIANCE (UK)

If your business handles personal data and information, you must make certain that you meet the legal requirements surrounding data protection. There are a number of laws that cover this area, though the most well known one is the General Data Protection Regulation (UK GDPR).

To help you understand what you can do to ensure that your business adheres to these laws we've put together this list of questions to ask yourself:

- **What personal data does your business hold?**

  You need to know exactly what information you have, how and where it is stored, where you got the information from initially, who it's shared with and what (secure) method you use to store it all.

- **Does your business need a Data Protection Officer?**

  For many small businesses this won't be necessary, although this will depend very much on the specific type of business you are running.

- **Do you know the rights that all people have with regards to their personal information and data?**

  There are eight in total and it's important that you and your staff are aware of them all. The eight rights are as follows:

  1. The right to be informed
  2. The right of access
  3. The right to rectification
  4. The right to erasure
  5. The right to restrict processing
  6. The right to data portability
  7. The right to object
  8. Rights in relation to automated decision making and profiling.

- **What policies does your business have that ensure you are able to respond to requests regarding the rights that individuals have?**

  It's important that you have policies and procedures for this and that your whole team is aware of them too.

- **Are you recording your actions regarding the handling of personal data?**

  Keeping a detailed record of any actions / decisions made regarding your processes and procedures re: obtaining consent, impact assessments, etc. as well as the information pertaining to how and when

you delete personal data.

- **Are you customers or clients aware of why you process and hold their personal data / information?**

  Answering this is key to ensuring you're in line with the rights that all people have with regards to their personal information and data mentioned above.

  You must inform your customers, clients and in some cases suppliers why you are processing and holding their personal data / information - ensuring that this isn't a 'one size fits all'\ approach either as you may be gathering data for different reasons from different people.

- **With regards to asking for consent, are you doing so to the standard required under the UK GDPR laws?**

  It's imperative that you include all of the relevant information within your request.

- **What will you do if there is a data breach?**

  Think through the steps you will take if this does happen. While we all hope that it won't happen to us, the fact is, it might do. Having a plan for if this happens will do two things:

  - Potentially highlight areas where you could make improvements to your data handling policies to help avoid breaches.
  - Minimise the effects of a breach by having a robust plan in place.

  Create a plan for what you will do in the event of a data breach and ensure that someone within your business is responsible for this.

- **Have you (and your staff) reviewed the UK GDPR's 6 guiding principles?**

  The six guiding principles are as follows:

  - Lawfulness, fairness and transparency.
  - Purpose limitation.
  - Data minimisation.
  - Accuracy.
  - Storage limitation.
  - Integrity and confidentiality (security)
  - Accountability.

  Further details regarding the UK GDPR's 6 guiding principles as well as further information on all of the above can be found on the ICO website: https://ico.org.uk/