# GDPR: Are You Ready?

SMEs: Summary High Level Checklist – refer to Information Commissioner's website for full details https://ico.org.uk/

| | | | |
|---|---|---|---|
| | | **GDPR AWARENESS** | |
| | | All staff and senior management are aware of GDPR and their responsibilities | Is awareness training recorded in Training log?<br>Training should be also included at induction and regular refresher training should be provided. |
| | | Principles of GDPR:- | Understand and embed them within your Organisation |
| | | a) Lawful, Transparent and Fair<br>b) Purpose limitation<br>c) Data minimization<br>d) Accuracy<br>e) Storage limitation<br>f) Integrity and Confidentiality<br>g) Accountability | <br>-Collected for specified, explicit & legitimate purpose<br>-Adequate, relevant and limited to what is necessary for the defined purpose<br>-Data is accurate kept up to date where necessary<br>-Kept in form that allows identification of personal data for no longer than necessary<br>-Appropriate security of personal data against accidental loss, destruction or damage<br>-The company executive is responsible and should be able to demonstrate compliance with all of the above. |
| | **1** | Who is responsible for managing compliance? | Data Controller or a Data Protection Officer if managing large volumes of data, or data defined as sensitive |
| | | **REVIEW OF SYSTEMS** | |
| | | Carry out an information audit and prepare information register | The ICO has provided templates that will be useful<br>**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/** |
| | | What personal data is being collected and is it special category?<br>For example, information about an individual's:<br>race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; sexual orientation or if the data is about a child under 16 (varies to under 13 by EU country) | Special category data is more sensitive and requires more protection, breach response processes. The loss of this data is treated more seriously by the supervisory authority (ICO). |
| | | Who is the Controller/Processor | Controller determines purposes and means of processing. |

| | | | |
|---|---|---|---|
| | | | Processor carries out specific instructions of controller for processing data under binding contract |
| | **2** | What is the lawful basis for having data:- | |
| | | a) Consent<br>b) Contract<br>c) Legal Obligation<br>d) Vital Interests<br>e) Public Interest<br>f) Legitimate Interests | If Legitimate interest basis used then a Legitimate Interest Assessment should be made to ensure that the organisations interests do not undermine the rights of the individual. |
| | | If Consent - how obtained/recorded? | Review marketing consent records. Is consent clear, specific, and freely given, have you got a traceable history of consent? |
| | **3** | Is it shared with any Third parties? | |
| | | Will it leave the European Economic Area (EEA) | If Data leaves EEA explicit consent will be required |
| | **4** | What is retention/deletion Policy? | |
| | | What is the location of personal data | |
| | **5** | How is data secured? | Encryption, technical controls, |
| | **6** | Rights of Data Subjects:<br>- To be informed<br>- Access<br>- Correction<br>- Erasure<br>- Restrict processing<br>- Object to processing<br>- To data portability<br>- Not to be subject to automated decision/profiling | |
| | | Privacy Notice at point of collection and include **1-5**<br>And how to exercise their rights under **6 -** and how to withdraw consent. | Privacy notice should be transparent include the identity and contact details of the controller and Data Processing Officer, purpose of processing, legal basis for processing, recipients or categories of recipients of the personal data, the right to lodge a complaint with the ICO and existence of profiling/automated decision-making |
| | | Have you a process in place to respond to data subject right to access within one month? | |
| | | Have you an incident response plan in place and have you tested it | Breaches need to be reported to ICO within 72 hours |
| | | Have you ensured that your 3rd party processors are GDPR compliant ? | Review 3rd party agreements and carry out due diligence, put binding contracts in place to extend to new individual rights support and breach reporting |

| | | | |
|---|---|---|---|
| | | Privacy Impact Assessment process in place for new processing activities involving personal data? | Article 25 – carry out assessment before new process implemented to ensure privacy by design and default |