GDPR
Q & A Fact Sheet

Address: The Workbox • 4th Floor • St. Mary's Terrace • PZ360 • Penzance • Cornwall • TR18 4DZ
Telephone: 0800 689 4168
Email: hello@cloudlegalsupport.com

- ✓ **What is the GDPR?** This is the 'General Data Protection Regulation' which replaces our Data Protection Act 1998 in the UK. It comes in to effect on 25th May 2018. It is the most important change to data protection and privacy law in two decades!

- ✓ **What is its main purpose?** The GDPR provides people with greater control and choice over their personal data and assurances that their information is being processed lawfully and securely protected. Trust and assurance between organisations and individuals is vital in this data driven world.

- ✓ **Who does it apply to?** The GDPR applies to all organisations (large or small) operating within the EU and to organisations that collect, store, use or share personal data pertaining to individuals located within the EU.

- ✓ **What is personal data?** Personal data is information relating to an 'identified or identifiable natural person'. Some examples include name, email, location data and IP address.

- ✓ **How does it impact your business?** You are either a Data Controller or a Data Processor in respect to any specific set of personal data. Whichever role you play, you have ***accountability*** and ***transparency*** obligations under the GDPR in respect of personal data which includes keeping records, lawful processing, secure storage and retrieval, breach notification, disclosure and more!

- ✓ **Am I a Data Processor or a Data Controller?** A processor is responsible for *processing* personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you. For example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure that your contracts with processors comply with the GDPR and that you obligate your processors to be GDPR compliant.

- ✓ **What rights do data subjects have?** A person, known as a 'Data Subject' has many rights in respect of their personal data including the right to: (i) be informed (privacy notice/ consent tick box); (ii) ask you to give them access to their personal data; (iii) have the processing of their personal data 'restricted'; (iv) have their personal data erased; rectified; ported and more…

- ✓ **Do I need to appoint a Data Protection Officer (DPO)?** The appointment of a DPO is mandated in certain circumstances i.e. where you (i) are a public authority; (ii) carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or, (iii) carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

- ✓ **Do I always need consent to process personal data?** No. Consent is one lawful basis for processing, but there are five others. Consent won't always be the easiest or most appropriate. You should always choose the lawful basis that most closely reflects the true nature of your relationship with the individual and the purpose of the processing. If consent is difficult, this is often because another lawful basis is more appropriate, so you should consider the alternatives. It's your responsibility to identify a lawful basis for processing under Article 6 of the GDPR.

- ✓ **What are the risks if I ignore the GDPR?** The GDPR is an *absolute* legal obligation i.e. it is not a choice to comply with it. Fines imposed can destroy a small business and significantly damage larger ones. Reputation will be damaged and without TRUST, a business may not survive. The ICO can undertake data protection audits on your business activities with little or no notice. Data subjects have enhanced rights too which if breached can result in compensation for individuals and class actions.

- ✓ **What can I do for my business to be compliant?** You need to start getting your business in order! Take control and accountability for your data processing activities to avoid a data breach now.

  Some things your business can do to be compliant include (i) carrying out a data mapping exercise; (ii) cleaning up what data you NEED to keep; (iii) putting in place 'appropriate technical and organisational measures'; (iv) reviewing and updating all GDPR/ IT Security documentation; (v) staff training; (vi) establishing internal processes for secure and lawful data processing; (vii) embracing a cultural shift within your business to support the fundamental right to privacy etc.

IT security, GDPR, training, support and cultural change are all essential ingredients to a wider business strategy

Step 1: It is suggested that you carry out a GDPR Audit. This will highlight what you are doing well and what you need to improve on or fix! Carrying out an obligatory GDPR audit will demonstrate that you take the requirements of the GDPR seriously, respect its objectives to apply freedom to privacy with regards to the protection of, and lawful processing of, a data subject's personal data. You might realise that you need to get certain GDPR forms, processes and policies in place to be operating effectively and lawfully.

Don't get caught out! Build up a mutual trust in your business. Get involved and own GDPR!