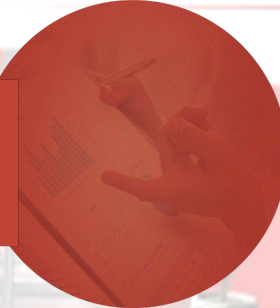# Is the UK ready for the EU General Data Protection Regulation in 2018?

£1,195,500 worth of Data Breach related monetary penalties issued by the ICO in 2016

and £1,026,250 in 2015

Source: ICO.org.uk

Human error consistently causes more data breaches than hacking but also enables hacking

1. Breach — April – Sept 2016 Biggest single data breach failure was 'Data posted or faxed to incorrect recipient'

2. Breach — April – Sept 2016 2nd biggest single data breach failure was 'Loss or theft of paperwork'

3. Breach — April – Sept 2016 3rd biggest single data breach failure was 'Data sent to incorrect email recipient'

GDPR QuickThink – a guide to support quality Data Protection and GDPR preparation

1. **Assess your current position** – carry out an audit to baseline current processing of personal data and sensitive personal data to the DPA98 as it stands now. Develop Data Flow diagrams showing the movement of such data within your organisation. This will show where data is held, who has access to it and enable legal requirements to be addressed.

2. **Review your data processes** – including security breach reporting, use of Data Protection Impact Assessments and review 3rd party contract clauses relating to data protection and information security.

3. **Review Data Protection documentation** - including relevant policies and notices such as Fair Processing Notices that include the additional rights of the Data Subjects.

4. **Ensure accountability** – Data Controllers are responsible for demonstrating compliance with the GDPR and so need to engage with the business's strategy in the medium and long term and make a record of how that is evidenced (documented). A good document management system is key to demonstrating accountability and ongoing compliance.

5. **Engage with Senior Management** - to prepare them for the likely implications regarding the GDPR's position on Extraterritoriality i.e. if monitoring or offering goods and services to EEA Data Subjects then GDPR applies regardless of where the company is based. Review and revise Insurance / Indemnities.

6. **Implement 'data protection by design' in software development** - for all planned systems that will process personal data that will meet the inherent requirements of the GDPR e.g. use of cryptographic techniques.

7. **Develop and implement staff training programmes** – to enable them to understand their own specific responsibilities in maintaining company compliance with the GDPR.

8. **Plan regular data protection audits** – at least annually to ensure continued compliance.

9. **Be transparent in your actions** – transparency builds trust so ensure both employees and customers know how you are processing their personal data and keeping it secure through robust security measures. Trust can assist businesses in gaining competitive advantage.

10. **Start planning now - the Regulation must be implemented no later than 25th May 2018 regardless of Brexit negotiations, which themselves won't complete until 2019 at the earliest.**