GDPR
Are you ready?

atradius
managing risk, enabling trade

GRAYDON
open in business

GDPR ....

- The General Data Protection Regulation (GDPR) is an important new piece of legislation adopted by the European parliament and the European council.
- Its purpose is to bring greater strength and consistency to the data protection given to individuals within the European Union (EU).
- The European Parliament and the European Council sees the regulation as an important part of its efforts to enable EU citizens to control the personal information which companies hold about them, while ensuring that companies themselves have a clear, straightforward and dependable set of rules to follow when handling personal information.

GDPR ....

- GDPR will come into effect on 25 May 2018 in the EU.
- All UK businesses will need to comply with the new legislation.
- It is crucial to ensure that your business is prepared.

GDPR ....

- There will be stricter rules around securing consent to use personal information.
- You will need to show that you have a crystal clear and definitive agreement from individuals to collect and hold their personal information and keep documented evidence to prove it.
- Companies will also have to demonstrate they have stated very clearly how they intend to process and then use the data they receive.
- The right to be forgotten will be introduced: organisations will not be allowed to retain individuals' personal information for any longer than needed.
- Will have to delete information if requested to do so.

GDPR ....

- The GDPR applies to all personal data – just like the UK Data Protection Act 1998 (DPA).
- Any information that is considered personal under the DPA will also be considered to be so under the GDPR. However, the definition in the GDPR is more detailed – referring to information such as genetic material as well as written data.
- The legislation highlights how changes in technology have changed the way data is collected by noting that online identifiers, such as IP addresses, can be considered personal data.
- Most businesses and organisations hold personal data that must be protected, some examples relevant include employee payslips, customer contact details, HR records and emails.

GDPR ....

- Fines for breaches under the rules of GDPR are €20 million or four percent of your global turnover
- Under the rules of the GDPR, organisations have a duty to report certain types of data breaches within 72 hours of the organisation becoming aware of it.
- These include breaches which are likely to result in risks to the rights of individuals, for example, if the breach is likely to cause an individual financial loss, reputational damage or breach of confidentiality.
- In some cases, businesses will also be required to report breaches to the individuals whose personal data has been compromised. These will be in cases where the risk to the individual's rights is much more significant.

GDPR ....

- Individuals Rights:-
  - To be informed - how data is being processed
  - To Access – able to obtain any data held
  - To Recification – correct any incorrect data held
  - To erasure – removal of any personal data held
  - To protect against automation decision making/profiling
  - To data portablility – resuse data held on them
  - To object – against direct marketing
  - To restrict processing – business can store data but not process if individual supresses use of their data

GDPR ....

- Implement appropriate technical and organisational measures that ensure and demonstrate that they comply
- Staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities
- Where appropriate, appoint a data protection officer
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include: Data minimisation; Transparency; Allowing individuals to monitor processing; and Creating and improving security features on an ongoing basis

GDPR ....

- The legislation comes into force in May 2018, organisations will be expected to comply immediately.
- It is therefore essential to prepare in advance so that you are ready to meet your requirements.
- It also means you have time to speak to legal counsel, data protection and information security specialists to ensure that any questions you have are answered.
- But more than that, a protected workplace is vital for every business to mitigate potential legal, financial and reputational risk.
- Organisations should ensure that all customer, employee and partner information is being managed, stored and disposed of securely.

GDPR ....

- Becoming compliant can be a time-consuming process as staff adapt to new responsibilities. It is therefore crucial to start implementing best practice as soon as possible so that once the GDPR comes into force, you are already up and running. Here are some actions to take.

  - Prepare a security policy and keepit up to date
  - Appoint a person/team to oversea data protection
  - Make it easy for staff to protect data with helpful policies
  - Train staff regularly

GDPR ....

Your thoughts, comments and concerns .....