*** RISK UPDATE FROM NTEGRITY***

By Gary Horswell – Managing Director

The new General Data Protection Regulations come into force a year from today, 25th May 2018. This is what you need to consider;

From the date the new GDPR comes into force, **all firms in all business sectors, regulated or not, will need to comply** and make significant changes to the way data is handled.

1. Ignoring GDPR is not an option

Companies not complying by this time next year face a tough new range of sanctions including:

- Fines of up to 4% of worldwide turnover to a maximum of €20,000,000,
- Audits, warnings and temporary, or permanent, bans on data processing,
- Individuals can sue a firm for compensation to recover material damage and distress.

Research by NCC Group (https://www.nccgroup.trust/uk/landing-pages/gdpr-impact-analysis/) reports that the new GDPR sanctions would have increased Talk Talk's fine from the ICO from £400,000 to £59m. Pharmacy2U, which was fined just £130,000, would have faced a demand for £4.4m.

2. Brexit will not mean we can forget GDPR

With the exit from the EU taking two years from March 2017, the UK will remain a member of the EU until 2019, after GDPR comes into force, so it will apply here.

Setting the 'equivalence' debate to one side, continuing to do business with companies within the EU after Brexit will almost certainly require the same approach on compliance.

3. Size of business doesn't matter

GDPR applies to all businesses, large and small, although the regulations recognise that smaller enterprises lack the resource of larger business.

Where can you obtain help?

The ICO has a launched website at https://ico.org.uk/for-organisations/data-protection-reform/ containing guidance and, as this is being updated continually, we recommend becoming a regular visitor.

Some of the main areas to consider;

Consent

One of the most challenging areas for compliance. Obtaining consent from an individual is one way (there are others) to justify processing their personal data but it will be much harder to obtain valid consent under the GDPR and individuals can withdraw consent at any time.

Obtaining consent to process sensitive personal data must be explicit. Consent to transfer personal data outside the EU must now also be explicit.

Data Subject Rights

Existing rights of individuals are largely preserved but there are some new rights including the 'right to be forgotten'.

Privacy Notices

The amount of information a firm needs to include in privacy notices has increased but the notices must still be concise and intelligible. Privacy notices are to apply from 25 May 2017 but guidance from the ICO may not be available until July 2017.

Accountability

Firms must not only comply with the six general principles listed but also be able to demonstrate compliance which is likely to mean more monitoring and auditing, following a re-write of procedures.

Data Protection Officer

This should not affect small and medium sized businesses and can be a voluntary appointment. Once appointed the DP officer must be involved in all data protection issues and cannot be dismissed or penalised for performing their role.

Data Security and Breaches

Firms are required to keep personal data secure. Data Controllers must report data breaches to the ICO (unless the breach is unlikely to be a risk for individuals) within 72 hours. Firms may also have to inform the affected individuals.

GDPR is a complex compliance challenge and careful forward planning, consulting with experts is essential in preparing UK businesses.

ENDS

This update is produced by Gary Horswell, MD of Ntegrity who are UK200Group Business Partners specialising in PII, cyber, directors & officers liability and other closely related areas too.

The UK200Group is a the UK's leading membership organisation of chartered accountancy and law firms proving its members with support in business development, delivery and risk reduction. Our members represent around 150,000 SMEs across the UK.

For more information on the UK200Group and our Campaign for Clarity on MTD, click here or visit www.uk200group.co.uk For Further information contact: admin@uk200group.co.uk