Change is on the horizon

On 25th May 2018, GDPR will come into full force across the EU

The General Data Protection Regulation is a huge new piece of EU legislation – one of the biggest and most significant changes to privacy legislation in the history of Europe. Long overdue, it constitutes a comprehensive overhaul of the EU's aging and outdated data protection laws, which were enacted in a time when modern advancements such as cloud technology, cookieless tracking and mobile browsing had not yet allowed for new ways of misusing and exploiting data. Specifically, GDPR will replace the current Data Protection Directive from 1995. Subject to much discussion and controversy, thousands of amendments were proposed along the way. GDPR was officially adopted in April 2016, and will have broad and far-reaching impacts on technology and businesses processes, both in Europe and further afield. Regardless of Brexit, the regulations will have a substantial impact on British organisations and remain relevant.

GDPR aims to strengthen data protection for all people within the EU, reinforcing the European notion that privacy is a fundamental human right. This law will reshape the way organisations approach governance of data while simultaneously giving people more control over how their personal data is used. It will also harmonise data privacy laws across the region (where previously each member country had its own set of rules), meaning that businesses will have a clearer, simpler legal environment in which to operate. All individuals and companies involved in the use of data in the context of selling goods and services to EU residents will have to abide by GDPR, regardless of where in the world they are located. GDPR applies to both data controllers and data processors, as well as to organisations who monitor the behaviour of EU data subjects. The regulations will be implemented by May 2018, when the grace period for compliance will come to an end. Furthermore, enforcement of this legislation is going to be robust, with considerable penalties for non-compliance. These penalties increase along a tiered scale in relation to the seriousness of the violation. Organisations who breach GDPR face fines of up to €20 million, or 4% of their previous annual global turnover - whichever is higher - meaning that the potential for loss of revenue is severe.

In order to understand what GDPR means for individuals and companies, its key aspects must be highlighted. The major standout points of GDPR cover several major areas, including a number of new individual rights which are codified under the legislation.

Key Points

- **Right to access** - An individual has the right to access their personal data, have it changed or corrected, and be informed of how it is being processed. “Personal data” covers PII (Personally Identifiable Information) such as name, address, contact information and bank account numbers, as well as data profiles (interests, buying patterns and habits) and lists of associated devices. Data subjects are also entitled to know how long their data is being stored for and who is able to view it.
- **Right to portability** - An individual has the right to be given their data. Data controllers are obligated to provide an electronic copy of personal data to data subjects if requested, for free. This allows people to reuse their personal data for their own purposes and transfer it across different IT environments. Data must now be stored in commonly-used formats, and requested moves must be undertaken within one month.
- **Right to be forgotten** - Also known as “right to erasure”. An individual has the right to have their personal data erased when it is no longer relevant to its original purpose. Data controllers are obligated to stop the distribution of such data if requested, and are responsible for informing other organisations to delete any copies (or links to copies) of that data.
- **Privacy by design and default** - This requires data protection measures to be purposefully entrenched in the development of businesses processes and throughout daily operations within organisations. Going forwards, when it comes to implementing new procedures and products, data protection must be included from the very outset.
- **Breach notification** - Organisations must inform their Supervising Authority of any data breaches they suffer within a 72 hour timeframe. Data controllers must also notify their customers of any risk of compromise. A personal data breach is defined as any breach of security which leads to unauthorised access or loss and destruction of PII.
- **Consent** - When obtaining consent for the use of data, organisations must use clear and easily understandable terms and conditions. Companies which profile and track individuals must get the individuals’ explicit consent to do so. Withdrawing consent must be as easy as it is to give it, and consent must be active on the part of the data subject, i.e. opt-in rather than opt-out.
- **Data Protection Officers** - Officers must be appointed to oversee data protection in all large organisations (over 250 employees) that engage in systematic processing or monitoring of personal data. These officers must be professionally qualified. DPOs will need expertise in security, project management and risk assessment in order to carry out their duties.

The clock is ticking. Start preparing for GDPR today.

So how can businesses ensure that they abide by these new rules and standards? They should begin by developing company-wide awareness of the law (at all employee levels), and allocating resources required for the compliance effort. Additional specialist staff or consultants may need to be brought on board.

Next, since good data hygiene is a central tenet of GDPR, businesses must become aware of what data they collect, how they use and manage it, and how this information flows through their organisational structure. Information audits, gap analyses and internal reviews of procedures and processes will need to be undertaken. Going forwards, maintenance of these systems will have to continue, as *ongoing* compliance is the overarching goal.