GDPR vs. UK DPA - THE KEY DIFFERENCES

The General Data Protection Regulation (GDPR) will replace the UK Data Protection Act 1998 (DPA) on 25 May 2018 but anyone that thinks this is a like-for-like swap is seriously mistaken. Although the underlying principles of the two pieces of legislation are similar, the changes brought in by the Regulation have significant ramifications. Crucially, GDPR introduces several new and demanding requirements for UK organisations that are likely to necessitate new policies, business processes and technologies.

In this article, the first of a three part series, we explore five key differences between the Regulation and the UK law that all businesses need to be aware of.

FINES

Currently, the Information Commissioner's Office (ICO) can issue fines of up to £500K to any UK organisation that "seriously breaches" the DPA. GDPR raises the stakes considerably. Organisations that fail to comply with the Regulation risk fines of up to €20m, or 4% of their annual global turnover - whichever is higher. Even minor infringements will result in fines of €10m, or 2% annual global turnover.

ACCOUNTABILITY

The concept of accountability underpins the DPA but it will become more important under GDPR. The Regulation contains an accountability principle, which requires organisations to demonstrate compliance through a series of actions, including the implementation of "appropriate technical and organisational measures".

Notably, organisations are also required to produce and maintain documentation that demonstrates actions taken to achieve compliance, e.g. easy-to-consume notices for customers that explain changes to data processing policies.

W | www.trust-hub.com E | hello@trust-hub.com T | +44 (0)20 3582 5055

BREACH NOTIFICATIONS

This all-new requirement puts pressure on organisations to reveal breaches at the earliest opportunity. Whereas the DPA doesn't require organisations to report data breaches, GDPR charges them to "notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it". The requirement also extends to notifying the individuals concerned if there is a high risk to their rights and freedoms.

RIGHT TO ERASURE

The 'right to erasure', or the 'right to be forgotten' as it's more commonly known, is well established but GDPR builds on this concept to give data subjects direct control over their personal details. Employees and customers now have the power to request the deletion or removal of personal data, and in certain circumstances businesses are obliged to comply. This right applies to both backups and archived data, as well as information shared with third parties. These organisations must be notified of the erasure request so they too can erase links to, or copies of, that information.

RIGHT TO PORTABILITY

Although the concept of data portability isn't new, GDPR introduces it into EU law for the first time with a new right for data subjects. This right enables individuals to obtain their personal data and reuse it as they wish. Organisations are obliged to comply with data portability requests providing the information in question meets a **specific set of criteria.** They must also present this information in a structured, commonly used and machine-readable format, e.g. CSV files, within a month of a request being issued.

That's all for now but join our **mailing list** for part two in this series, which will be available next month. Discover how GDPR affects data processors and find out if you need a Data Protection Officer. We'll also explore what expanded definitions for consent and personal data mean for your business.

In the meantime, **visit our website** to learn more about the challenges and opportunities presented by GDPR.

W | www.trust-hub.com E | hello@trust-hub.com T | +44 (0)20 3582 5055