Becoming GDPR Compliant

Notes and guidance on preparing for the GDPR

With less than 200 days to go until GDPR becomes enforceable, the pressure is on for companies and other organisations to become compliant before the deadline of 25th May 2018. Alarmingly, there are recent signs that a significant number of businesses are still unprepared – in September 2017, a survey by law firm Blake Morgan found that 9 out of 10 businesses had still not made critical changes to their privacy policies, and in November, a survey conducted by trade body DMG Group revealed that 40% of marketers in the UK felt that their businesses were not yet ready. With the potential for towering fines and the scale of change required, companies must implement a plan for GDPR compliance as soon as possible.

Awareness

Not everyone is aware of GDPR; outside of IT departments, individuals may know about the change but not appreciate how significant it is or realise the impact it will have. Initially, key people within an organisation – board members, management, decision-makers and resource allocators – should all be well-versed in what GDPR encompasses. Later, all employees should be brought up to speed through training across the business.

Data Mapping & Privacy Policies

As a foundational activity, companies must also become aware of what information they hold. All sensitive personal data stored should be documented, including details about its origin, where it is held and with whom it is shared. One way of doing this is through an information audit. This involves asking questions about how the business processes personal data and how client-facing representatives obtain customer details. Data mapping (the process of identifying, understanding and mapping out the data flows within an organisation) can contribute to the development of a comprehensive overview of these facts and findings. Since GDPR dictates that privacy information must be given to data subjects when their personal data is collected, it is imperative that companies take stock of their existing privacy policies and notices, and check if these will need to be updated.

PII & Access Requests

Further procedures requiring internal review will include those pertaining to the rights of individuals, and subject access requests. Indeed, all such processes and codes of conduct will need to be held up, critically examined and checked for adherence to GDPR. Comparing

them in this manner will serve to highlight inadequate areas and identify any 'missing pieces' (a form of gap analysis). Businesses should carefully consider their system architecture and all relevant third party data processors. In addition, they will need to ensure that they are capable of swiftly responding any requests for Personally Identifiable Information (PII) i.e. access requests. Right to data portability (an enhanced form of subject access) is an entirely new right that will need to be accounted for; organisations should come up with a way of providing such data in a manner which meets common industry standards. The existence of a Subject Access Request Register is therefore an important box to tick here. It should be noted that for companies which process a vast quantity of requests, logistics may become an issue. In these cases it would be advisable to consider automation i.e. developing online access systems, in order to reduce administrative strain.

Consent & the Law

A combined approach on both technological and procedural fronts will be key when it comes to achieving compliance, as there is no 'magic bullet' solution. Businesses should document their legal grounds for processing personal data; start keeping records of their assessments of these legitimate interests; and when consent is the basis for processing, ensure that it was captured in a compliant way. GDPR's significant shift in the role of consent means that organisations will have to review their tactics relating to obtaining and recording consent. For many, it will mean a move away from their current opt-out consent models, and adopting the required opt-in approach. And when it comes to consent and children, special steps will also need to be followed – for example, privacy notices aimed at children will have to be written in clear and child-friendly language.

Data Breaches

Furthermore, recent high-profile data breaches show how critically important it is for businesses to reinforce their cybersecurity and ensure that they are equipped to handle any data breaches. Breach notification duty will be new to many organisations, but regardless they should adopt robust internal processes for detecting, reporting and investigating personal data breaches. This may involve implementation of enhanced incident response procedures, and investigating measures such as encryption, pseudo-anonymisation and data masking. It is highly recommended that companies create and maintain an internal breach register and identify their Lead Supervisory Authority (e.g. the ICO for U.K.-based companies). Protection Impact Assessments will also be valuable in this arena, particularly when it comes to high-risk situations.

DPOs

A plethora of such assessments, toolkits, checklists, analyses and other preparation roadmaps are available on the market. Independent specialists with the right skills are now in high demand but short supply. This is because an essential stepping stone to becoming compliant for many larger companies will be to designate or employ a Data Protection Officer. DPOs can be from within or out with the organisation, but as it is such an important role, they must have suitable and relevant experience.

Different staff and different departments will have different roles when it comes to ensuring compliance. It is important to note that getting ready for GDPR cannot just be the remit of IT. There is no definitive way to prepare, and the aspects discussed here are by no means exhaustive. Firms will have to be thorough in devising a plan to tackle such issues, and adopt a multi-pronged strategy. Taking action and making GDPR preparation a top priority now will serve to protect against serious financial and legal consequences in the future.