ADEPT 4

IT AS A SERVICE

10 GDPR Misconceptions

1 *Isn't GDPR just an updated version of the Data Protection Act (DPA)?*

The General Data Protection Regulation legislation not only acts as an update to the Data Protection Act (which will be 20 years old in 2018) but extends this by protecting personal data subject rights. Data processors and controllers must keep these subjects informed on how their data is being used. There are six principles in total: lawful, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitations; and, integrity and confidentiality which will replace the eight principles covered by the DPA.

I'm DPA compliant so surely I'm already GDPR compliant? 2

The GDPR principles are far more prescriptive than those used in the DPA demanding accountability, privacy by design and setting out requirements for Data Privacy Impact Assessments (DPIAs) and the appointment of a Data Protection Officer (DPO), among other things. The legislation extends the rights of the data subject to allow data to be suspended, corrected, amended, or erased on request. It places the onus on the data controller and data processor to demonstrate compliance with the principles by recording processing activity and the actioning of requests. Therefore DPA compliance does not equate to GDPR compliance.

3 *Do we need to start from scratch to meet the GDPR?*

There are commonalities between GDPR, the DPA and other standards that could save you considerable time and effort. If you are DPA compliant its worth performing a gap analysis to work out where you need to make changes. In addition, those organisations that are ISO 27001 compliant will already have some of the documentation in place required to demonstrate accountability. The ISO27K Forum has mapped ISO 27001 against the GDPR here.

Does GDPR only apply to customer data? 4

The legislation covers a far broader range of data or Personally Identifiable Information (PII) and applies to all personal data including that held on employees. This means that even data held internally, such as that used by the Finance and HR departments, will be subject to the same rules in terms of transparency, integrity, confidentiality and accessibility.

5 *Do I have to obtain explicit consent?*

Explicit consent and consent vary and you don't necessarily need either. You can look at using another lawful basis to justify processing. There are six lawful bases listed in Article 6(1) of the GDPR and consent is just one of them. However, obtaining explicit consent does make it far easier to justify certain types of processing such as restricted processing, automated decision making or overseas transfers in the absence of adequate safeguards. If you do use consent as the basis for lawful processing be aware that this means data subjects can exercise their rights to access/amendment/erasure etc.

6

Must I appoint a Data Protection Officer (DPO)?

Only organisations that are either a public authority or public body or who monitor large numbers of individuals systematically or process large volumes of sensitive personal data are required to appoint a DPO. This applies to both data processors and data controllers. You can voluntarily appoint a DPO which will help with accountability but in doing so must observe the conditions laid down. These stipulate the DPO must have 'expert knowledge of data protection law and practices', oversee DPIAs, make their contact details known to the ICO and publish these, and be able to operate without impunity.

Will a data breach result in a hefty fine?

The maximum fine which the ICO can impose is set to increase from £500,000 under the DPA to €20,000,000 or 4% of an organisation's annual global turnover (whichever is greater). Large fines will be applied to organisations that breach consent requirements and/or retain data unnecessarily. To avoid these fines, organisations need to demonstrate accountability by documenting data processing to prove transparency. Fines can also be avoided in the event of a breach by ensuring tried and tested response processes are in place to notify data subjects and/or the supervisory authority.

7

8

Do I still have control over my data?

GDPR rewrites the rules when it comes to data ownership. The data subject is now able to monitor processing and request data is amended, suspended or erased. The data controller still has to observe data minimisation and data retention requirements in common with the DPA but now has far greater responsibilities for the protection of that data by implementing privacy by design in its technology and processes. So ensuring data is housed securely, perhaps by taking it into a secure cloud or virtual environment, ensuring that access is authenticated, and ensuring that data is encrypted and key management is secure, for example.

Is the GDPR a mandatory standard?

While GDPR is a mandatory piece of legislation developed by the EU and converted into UK law by the Data Protection Bill, it is not a standard. There are expectations that a standard will shortly follow which is often referred to as the Privacy Seal and the expectation is that companies who demonstrate compliance will be able to display this seal.

9

10

Isn't GDPR just about applying more technical controls?

To become GDPR compliant you need to go through a process that entails mapping the people, the processes, the data locations, and the types of data that are used within your organisation. Only then can you begin to look at applying security controls to mitigate risk to that data, such as access control, anonymization and encryption. So while security is important, which is why the regulations call for privacy by design and by default, GDPR readiness is all about assessing and identifying those assets and processes and getting policies in place before you look at the controls required.