GDPR

The General Data Protection Regulation (GDPR) will replace the UK Data Protection Act 1998 (DPA) on 25 May 2018. 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.

GDPR v DPA

Fines

Currently, the Information Commissioner's Office (ICO) can issue fines of up to £500K to any UK organisation that "seriously breaches" the DPA. Under GDPR, 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. While this is unlikely this will affect DIO to any great extent[1], a 'breach' remains highly undesirable.

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.

DIO must understand for each system it oversees whether it is the Data Controller or Data Processor, as each now has responsibilities and the demarcation lines for shared responsibility for security need to be identified and addressed.

Breach Notification

GDPR requires 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. DIO needs to identify its processes for incident notification and where necessary strengthen them.

Right to Erasure

The 'right to erasure', or the 'right to be forgotten' as it's more commonly known, is well established, though the DPA does not mandate it. GDPR builds on this concept to give each data subject direct control over their personal details. Employees and customers now have the power to request the deletion or removal of personal data,

[1] Article 79 says that penalties for violations should be effective and proportionate and it is probable that the UK ICO will be less stringent than GDPR allows.

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 (industry Partners). Industry Partners must be notified of the erasure request so they too can erase links to, or copies of, that information. While MOD in general, and DIO in particular have many legal obligations (i.e. for IMS, financial data must be kept for 7 years) to deny data subjects this right, it will be necessary to check and reaffirm this against GDPR and document the processes required where erasure applies.

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. Does DOI hold data that data subjects would desire to extract machine-readable copies of?

Privacy by Design

Article 22 of GDPR instructs Data Controllers to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance. Article 23 sets out principles of privacy protection by **design** and **default.** This not only includes security by design, but data subject's access rights by design (dependant on technology available and cost).

Consent

The need for consent underpins GDPR. It must be explicit, unambiguous and unequivocal. Individuals must opt in whenever data is collected and there must be clear privacy notices. These notices must be concise and transparent and consent must be able to be withdrawn at any time.

Privacy Impact Assessments v Data Protection Impact Assessments

While PIAs were not required by the DPA, they are mandated by the Cabinet Office and DIO has PIA's for the majority of its systems. Article 23 of GDPR requires Data Controllers to conduct a Data Protection Impact Assessment for all high-risk processing activities. The 'is it high-risk' question is answered by the preliminary pre-PIA questionnaire. The other important question is whether the PIA answers all the questions posed by GDPR. A gap analysis on each PIA is required and it is probably best that these are re-written as DPIAs. As Data Controller for many systems operated by Industry Partners, a review of their PIAs, if any and a quality analysis might also be required, Industry Partners must be aware of their responsibilities as Data Processors.

Suggested Strategy

Initiate the type of activity briefly listed below.

- Initial System Catalogue – Quantify the Task in Hand.
- Create a Governance Framework.

- Create Project Team.
- Draft DPIA.
- Compare with existing PIAs.
    - Data Landscaping of all major Systems.
    - Engage System Owners.
    - Analyse Data Sets.
    - Classify Data.
    - Map data to locations / systems.
    - Privacy Risk Assess – quantify the likelihood and severity of a negative impact on a data subject's rights.
    - Review Controls – list Gaps.
- Draw up action plan.
    - List Objectives.
    - Assign Owners.
    - Record Timescales.
- Internal Audit.
- Corrective Actions.

Justified and Legal non-compliance

For each of your 'high-risk' processing systems there are many reasons, legislative, regulatory and defence-of-the-realm type issues, why you cannot be compliant with the spirit of GDPR and there are many provisos in the regulation itself. To balance these requirements consistently and appropriately, you will have to seek advice from legal experts.