Miss IG Geek Ltd
thinking human

# Data Protection Roadmap

## How Miss IG Geek can help

Many organisations attempt to tackle their data protection management programmes by diving straight into tactical fixes, such as writing procedures or tweaking settings. However, in the absence of any top-down, strategy-led framework for data protection management, these efforts can quickly become irrelevant as the organisation evolves and adapts. By starting the approach to data protection with strategy and governance instead; an organisation can ensure that effort and resources are directed appropriately and can be managed within business-as-usual activity, even after the initial catching-up period has been left behind.

### 1. Developing data protection strategy and governance:

#### 1.a. Objective-setting

- What position and level of maturity is the organisation aiming for?
    - *In what timeframe*?
- How is risk appetite determined, monitored and decided upon?
    - *Who has the ultimate authority over data protection decisions*?
- Who at the executive level will supervise the organisation's data protection management programme?
    - *Does the organisation need a statutory DPO*?
- Will the organisation invest in internal data protection expertise, or rely on outside help?
- What level of priority will data protection be given in the management stack?
- How will progress/divergence be monitored?

➔ Establish strategy and formulate policy

---

***I can help with:***

- Workshopping DP strategy or providing materials for the organisation to determine this internally
- Assessment of whether a statutory DPO is required
- Identification of risks and issues
- Assistance with ICO registration
- Reviewing policy documentation

---

### 2. Discovery and intelligence-gathering

After, or in parallel with establishment of the organisation's 'ground rules', the finer details of the organisation's processing activities can be addressed. While some practitioners advocate starting with automated data discovery, others may prefer to investigate business process, or data subject journeys in order to identify and match data assets with purposes. There are pros and cons to either approach, and the 'best' one largely depends on the particular organisation and its circumstances. The information all needs to be generated and collated at some point, so it doesn't really matter which end it is tackled from.

Miss IG Geek Ltd
thinking human

### 2.a. What does the organisation do that involves processing personal data; why and how?

- Identify processing activities, purposes, data types, data subject categories, lawful bases, transfers, systems, acquisition points.
- Where is high-risk processing occurring?

➔ Record of Processing Activities (ROPA)-building

---

***I can help with:***

- Defining purposes of processing
- Identifying appropriate lawful bases
- Risk assessment of processing

---

### 2.b. How much of a gap?

- ...between what's in place now and what the organisation will need to reach their target position and maturity? (Process, knowledge, documentation, mechanisms, resources, etc)
- ...between paperwork and reality?

➔ Gap/risk analysis

---

***I can help with:***

- *Conducting gap analysis of process, knowledge, documentation etc*
- *Advising on workstream priorities to support strategy*

---

## 3. Programme planning and management

### 3.a. Establish the basics

- Foundational training for all staff on terms and concepts of data protection.

---

***I can help with:***

- Supplying learning sessions, remotely or in person
- Guidance and info materials

---

### 3.b. (Re-)Engineer processes to integrate requirements for:

- Data subject rights
- Data protection risk assessment
- Data protection by design and by default (DPbD2)
- Authority and accountability controls

➔ Documentation, communication, implementation

---

***I can help with:***

- Providing advice on logistics of processes for upholding DS rights
- Being an outsourced provider of risk assessments
- Providing training and resources about DPbD2 (including DPIAs)
- Reviewing documentation
- Assessing lawfulness of ex-EEA transfers

---

### 3.c. Close gaps as necessary for the organisation's desired position and maturity

- Further data protection training/support for specialist roles (eg, HR, sales/marketing, ICT)
- Upgrade privacy info to reflect ROPA content
- Review relationships (contracts, agreements, supply chain) and remedy defects
- Update and organise documentation

---

***I can help with:***

- Delivering specialist training
- Producing, or assisting with privacy info materials
- Review of DP terms in contracts

---

All of the service and support options outlined in this document can be delivered remotely; some by email correspondence alone. Workshops and training session tend to be more effective when delivered in person, however due to the impact of Covid-19, direct face-to-face meetings may not be feasible.

Every 'how I can help' activity can be delivered as a separate, stand-alone piece of work, although there are some dependencies – for example, drafting privacy notices requires information that must already be present in the ROPA.