The Information Commissioner's powers

Data protection incidents which occurred prior to 25 May 2018 fall under the Data Protection Act 1998 (the DPA 1998) which was in place until that date.

Incidents which occurred on or after 25 May fall under the General Data Protection Regulation (the GDPR) and/or the Data Protection Act 2018 (the DPA 2018), which we refer to as the 'data protection legislation', depending on the nature of the processing involved.

There are a number of powers available to the Information Commissioner's Office (ICO) in respect of breaches of the data protection legislation.

Our powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

The main options are to:

- provide practical **advice** to organisations on how they should handle data protection matters;
- conduct **consensual assessments** (audits) to assess whether an organisation's processing of personal data follows good practice;
- issue **information notices** requiring individuals, controllers or processors to provide information as part of an investigation into compliance with the data protection legislation. If the recipient of an information notice does not provide a full and timely response, the ICO may apply for a court order requiring compliance with the information notice;
- issue **assessment notices** to allow us to investigate whether a controller or processor is compliant with data protection legislation. The notice may, for example, require the controller or processor to give us access to premises and specified documentation and equipment;
- issue **warnings** where proposed action threatens non-compliance with data protection legislation;
- issue **reprimands** for infringements of relevant data protection legislation;
- issue **enforcement notices** where there has been an infringement, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the data protection legislation;

- issue **penalty notices** requiring organisations to pay administrative fines of up to 20 million Euros, or in the case of an undertaking, up to 4% of the total worldwide annual turnover, depending on the nature of the infringement; and

- **prosecute** those who commit criminal offences under the data protection legislation. In Scotland, where the ICO is satisfied that there are grounds for a prosecution, it will make a report to the Procurator Fiscal to make a determination whether or not to prosecute.

The ICO are also the Competent Authority for Relevant Digital Service Providers (r-DSPs) under the Network and Information System Regulations (NIS regulations).

The NIS regulations came into force on 10 May 2018 and aim to establish a common level of security for network and information systems. These systems play a vital role in the economy and wider society, and NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks.

There are a number of powers available to the ICO in respect of breaches of the NIS regulations.

- **Information Notices:** requiring an r-DSP to provide information to enable the ICO to assess the security of it's systems and the implementation of its security policies;
- **Powers of Inspection:** to assess if an r-DSP has fulfilled its requirements in identifying and taking appropriate and proportionate measures to manage the risks posed to organisations who provide an online marketplace, online search engine, or cloud computing service;
- **Enforcement Notices:** may be served if;
    - the r-DSP has failed in taking appropriate and proportionate measure to manage risk;
    - Failed to report a NIS incident;
    - Failed to comply with the notification requirements of NIS;
    - Failed to comply with an Information Notice;
    - Failed to comply with a direction given by the Commissioner.
- A **Penalty Notice** may only be served after the issue of an Enforcement Notice under NIS when;
    - The r-DSP was instructed to take steps to rectify a failure and failed to do so;
    - Or the Commissioner is not satisfied by the representations made by the r-DSP in regards to their response to an Enforcement Notice;
    - There are three tiers of penalty notice ranging from £1million to £17 million.

The Commissioner is also responsible for ensuring organisations comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended. These regulations establish rules by which organisations that engage in electronic marketing to individuals must comply.

To ensure this the Commissioner has the power to

- Provide practical advice and guidance;
- To issue third party information notices in order to identify organisations that are sending unsolicited marketing communications;
- Issue information notices compelling organisations to answer questions regarding their processes;
- Issue both enforcement notices to ensure future compliance and monetary penalties up to a maximum of £500,000 in response to previous non-compliance with the Regulations.

The Regulations also place an onus on communications service providers to notify the Commissioner of any security breach with 24 hours of the breach being detected. Failure to comply with the reporting timescales can result in a fixed fine of £1000 being issued.