Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

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. For more information about our powers under the DPA 1998 please see the accompanying document 'ICO Enforcement leaflet - DPA 1998'.

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.

Information about our chosen approach to regulatory action can be found in ICO's draft Regulatory Action Policy which gives direction and focus to the organisations it regulates.

Information about action we have taken can also be found on our website:

https://ico.org.uk/action-weve-taken/