Regulatory Panel terms of reference

1. Purpose

1.1. The Panel's purpose is to make independent recommendations to the Commissioner regarding proposed regulatory action as a result of breaches of legislation by data controllers or data processors. This includes recommending to the Commissioner the range of fines and other corrective measures which it would consider to be appropriate.

1.2. The Panel will usually advise the Commissioner on cases relating to breaches of the Data Protection Act 2018 (DPA18), General Data Protection Regulation (GDPR) or Network Information Systems (NIS) regulations, where the ICO's Penalty Setting Meeting (PSM) recommends a fine in excess of £1m.

1.3. The Panel will not consider cases in relation to any other legislation which the ICO regulates[1].

1.4. The Commissioner may choose to consult the Panel on other regulatory action under DPA 18 (and GDPR) or NIS where appropriate.

1.5. The Panel is advisory and makes recommendations to the Commissioner. The Commissioner remains the regulatory decision maker.

2. Responsibilities

2.1. To fulfil this purpose, the Panel convenes after a Notice of Intent (NOI) for a fine of over £1m has been issued and, at that meeting, is responsible for:

- considering whether the fine (and any corrective measures) is necessary, proportionate and justified. It will do this by:
  - assessing the evidence in the case;

[1] Privacy and Electronic Communications Regulators 2003; Freedom of Information Act 2000; Environmental Information Regulations 2004; Infrastructure for Spatial Information in the European Community Regulations 2009; Re-use of Public Sector Information Regulations 2015; Investigatory Powers Act 2016; Electronic Identification and Trust Services for Electronic Regulations 2016.

- applying all relevant considerations of the legislation being applied;
- taking into account the recommendations of the Penalty Setting Meeting to the Commissioner;
- where appropriate, considering whether the action is consistent with previous regulatory action taken by the ICO; and
- considering representations from organisations regarding the NOI.

The Panel will then recommend to the Commissioner the range of fine and other corrective measures which it would consider to be appropriate.

2.2 On a regular basis, the Panel will take steps to review the consistency of the ICO's regulatory action.

2.3 The Panel will not usually meet when Article 60 of GDPR (or other similar legislation) applies to the case in question. The Commissioner has determined that the Article 60 process provides sufficient independent scrutiny and advice on proposed regulatory action that additional input from the Regulatory Panel is not required.

3. Authority

3.1. The authority for the Panel derives from the Commissioner. However, the Panel makes recommendations and has no decision-making power.

4. Composition

4.1. Each meeting of the Panel comprises three members, drawn from a pool of potential members. Members are appointed to this pool by the Commissioner. The membership pool will be a mix of:

- A Non-executive Director of the ICO's Management Board, who will chair the meeting;
- ICO staff (at Level G2 or above); and
- External members as subject matter experts. This may include, but is not limited to, members of the ICO's advisory panels[2].

4.2. Members for each meeting of the Panel will be selected based on the areas of expertise required to consider the case and panel member availability.

[2] E.g. Technology advisory panel

4.3. ICO staff representatives on any Panel will not have been involved in, or responsible for, any part of the investigation of the breach. Panel members will be asked to make a declaration of this at each meeting.

4.4. All members of the pool are considered to be an agent of the Commissioner and as such are subject to the provisions within section 132 of the DPA 18 regarding confidentiality of information.

4.5. All potential panel members will be advised of the cases that will be considered at each meeting and required to disclose any potential conflicts of interest with respect to the parties involved in each case.

5. Quorum

5.1. All three members of the Panel must be present for the meeting to be quorate. Members may attend the panel virtually (e.g. by video or teleconference).

6. Information requirements

6.1. The Panel should ensure that arrangements are in place to enable it to discharge its responsibilities effectively, including the timely provision of information in an appropriate form and quality.

7. Budget

7.1. The Panel has no budget. Any spending required will be funded from the relevant Service's budget.

8. Secretariat

8.1. Secretariat is provided by the Corporate Governance Team.

8.2. Secretariat will produce a record the Panel's recommendation to the Commissioner and the reasoning behind it.

9. Frequency of meetings

9.1. The Panel will meet whenever required by the ICO's regulatory action.

10. Evaluation

10.1. The Panel should ensure that arrangements are in place to enable it to discharge its responsibilities effectively, including a regular formal evaluation of the Panel's performance.

11. Links to other forums

11.1. The Panel will report directly to the Commissioner.