Explanatory Framework for Adequacy Discussions

Section G: The Role of the ICO and Redress

Overview

This section explains how the ICO is a strong, independent, and effective data protection authority. It sets out the ICO's powers and responsibilities, its governance and independence, including its staffing, funding and spending, and its effective enforcement and compliance regime. It also outlines the administrative and judicial redress systems that enable individuals to pursue legal remedies to enforce their rights rapidly and effectively.

Section G: Role of the ICO and Redress

PART I - INTRODUCTION TO THE ICO

The Information Commissioner's Office (ICO) is the UK's independent data protection supervisory authority. The ICO is tasked with monitoring, ensuring, and enforcing compliance with data protection and privacy provisions, including handling complaints from data subjects. It is one of the largest data protection authorities (DPAs) in Europe and has:

- **Over 720 staff**, rising to 825 by 2020-21;
- A **budget of £51.4 million** (€55.65 million) for the financial year 2019-20, almost all of which supports data protection compliance.

It has had an excellent track record as an independent and effective regulator since 1984, tackling complex cases, and taking a proportionate approach to enforcement, including issuing substantial fines when necessary.

The ICO has a **wide range of powers to enable it to be an effective data protection authority**. Many of these are similar to powers in the Data Protection Acts 1984 and 1998. As the ICO's responsibilities have increased significantly in recent years, the DPA 2018 extended various existing powers and created new ones to help the ICO effectively fulfil these new responsibilities. The ICO's powers mean it can:

- Require **certain information from controllers or processors** within a specified time period. This has been extended to cover people other than a controller or processor. The ICO can also ask a court to order compliance with an information notice;
- Serve assessment notices on controllers or processors **to provide evidence of their compliance, which may include providing access to their premises**. The ICO is also able to carry out **"no notice" inspections** in certain circumstances;
- Serve **enforcement notices** where there has been an infringement, requiring organisations to take, or refrain from taking, specified steps to comply with the law;
- **Levy monetary fines** for breaches of data protection legislation or failures to comply with enforcement mechanisms. Under the UK GDPR, **fines can be as high as 4% global turnover or £17.5 million**, whichever is highest;
- **Prosecute those who commit criminal offences** under the DPA 2018, or refer cases to the appropriate prosecutor. The Act includes a new offence for deliberately destroying or concealing evidence identified as being relevant to an investigation.

These enforcement powers are set out in more detail in Part II of this section.

The ICO's other tasks include:

- **Advising Parliament, the Government, and others** on legislative and administrative measures relating to the processing of personal data;

- Providing **advice on data protection impact assessments** of processing that is likely to result in a high risk to individuals;
- Issuing a controller or processor **with a reprimand** where processing has infringed UK data protection law, and a warning where processing appears likely to do so;
- **Approving binding corporate rules** in accordance with Article 47 of the UK GDPR;
- **Encouraging and regulating data protection certification mechanisms**. This includes approving criteria for certification; accrediting bodies; carrying out periodic reviews; and withdrawing certifications no longer meeting the necessary requirements;
- **Producing various statutory codes of practice**, e.g. data-sharing, journalism processing, direct marketing, age-appropriate design;
- **Encouraging the drawing up of codes of conduct**; issuing opinions and approving draft codes of conduct, publishing requirements for monitoring bodies, and accrediting bodies to monitor compliance with codes of conduct.

The ICO is also empowered to take various regulatory actions for breaches of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)[1], and various other pieces of legislation[2].

The remaining parts of this section cover:

- Part II: The ICO's investigation and enforcement powers;
- Part III: The ICO's independence, and governance arrangements;
- Part IV: The ICO's activities providing guidance and advice;
- Part V: The ICO's role and activities in the international sphere;
- Part VI: Data subjects' ability to seek a judicial remedy instead of, or in addition to ICO action, and their ability to complain about ICO service.

[1] S.I. 2003/2426.

[2] Freedom of Information Act 2000 (FOIA); Environmental Information Regulations 2004 (EIR); Environmental Protection Public Sector Information Regulations 2009; Re-use of Public Sector Information Regulations 2015; Enterprise Act 2002; Network and Information System Regulations 2018; Regulation (EU) 910/2014 as it has effect in EU law and SI 2016/696.

PART II: INVESTIGATION AND ENFORCEMENT POWERS

The ICO has a number of tools available to ensure compliance and has a strong track record of using them to be an effective enforcer. A 2017 report found that the ICO has been among the top three European data protection authorities most active in recent years in terms of individual fining decisions.[3]

This section outlines the various powers the ICO has at its disposal. It covers:

- The power to issue information notices, assessment notices, enforcement notices, and penalty notices. It also covers what factors the ICO takes into account when deciding to issue such a notice, and appeal routes;
- The power to prosecute various criminal offences under the DPA 2018; and
- Examples of recent enforcement activity, both in terms of issuing fines, and prosecuting criminal offences

Information Notices

The ICO has the power to issue **information notices** under section 142 of the DPA 2018[4]. An information notice may require a controller or processor to provide information that the ICO reasonably needs for carrying out their data protection functions.

Information notices may also be given to "any person" to provide information that is reasonably required:

- To determine whether the personal or "household exemption" applies; or
- For investigating an offence under the DPA 2018 or a range of compliance failures. This range is set out in section 149(2) of the DPA 2018.

The ICO's Regulatory Action Policy[5] sets out the criteria it uses to determine whether it is appropriate and proportionate to issue an information notice. The criteria are:

- The risk of harm to individuals, or the level of intrusion into their privacy potentially posed by the events or data processing under investigation;
- The utility of requiring a formal response within a defined time period;
- The utility of testing responses, by the fact that it is an offence to deliberately or recklessly make a false statement in a material respect in response; and
- The public interest in the response.

[3] Nemitz, Paul Friedrich. (2017). Fines under the GDPR. CPDP 2017 Conference Book. Available at: SSRN: https://ssrn.com/abstract=3270535.
[4] Specific provisions for information notices are set out in Sections 142-145 of the DPA 2018, including restrictions on this power.
[5] ICO. Regulatory Action Policy. Available at: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

Section G: Role of the ICO and Redress

Sometimes the ICO may need to issue "urgent" information notices to obtain information quicker. In such a case, the ICO must still allow at least 24 hours for the recipient to respond. When deciding the period for compliance with information notices, including whether to issue an urgent notice, the ICO will consider:

- The extent to which **urgent investigation may prevent or limit the risk of serious harm to individuals** or serious intrusion into their privacy. For example, the ICO may need an early report on a serious data security breach in order to advise the controller on appropriate notification to data subjects and mitigation of the breach;
- The extent to which **urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence** of data processing;
- The **scope of the notice**, i.e. the scope of the questions or requests;
- The **additional burden** on the recipient from having to urgently comply with a notice;
- The **impact on the rights of the recipient**, should the ICO obtain information under an urgent information notice (which may be by court order), prior to an appeal being heard by the Information Tribunal against the information notice itself;
- The **length of time** of the investigation. For example, it may be appropriate and proportionate to issue an urgent information notice during a long running investigation, where the questions are limited and the response may bring the investigation closer to completion; and
- The comparative **effectiveness of the ICO's other investigatory powers**.

If a recipient of an information notice does not fully respond within the time limit, whether urgent or not, the ICO will endeavour to promptly apply for a court order requiring a response. In some cases, the ICO may decide not to make such an application. Among the criteria used to reach this decision are:

- The reasons for non-compliance with the information notice;
- Any commitments given by the recipient to responding to the information notice;
- Whether the information has been, or is likely to be, obtained from another source;
- The comparative effectiveness of other investigatory and enforcement powers of the ICO. For example, the ICO may decide it has sufficient evidence to move to an enforcement action in any event; and
- The public interest.

The ICO will also consider whether or not to issue a penalty notice for the failure to respond. This type of notice is outlined further below.

Assessment Notices

An assessment notice is a notice issued by the ICO to a controller or processor **requiring them to allow the ICO to carry out an assessment of their compliance** with data protection legislation.[6]

For example, an assessment might include how the data controller or data processor:

- Ensures its processing is fair and transparent;
- Obtains and maintains personal data;
- Ensures the confidentiality, integrity, and availability of the data;
- Retrieves and uses personal data;
- Responds to requests from data subjects exercising their data protection rights;
- Discloses personal data to third parties; or
- "Weeds and destroys" personal data.

The ICO can set the parameters of an assessment. This can include requiring access to premises; viewing information held on the premises; being provided with copies of information, and observing processing activities. As part of an assessment, the ICO may also require the data controller or data processor to make available for interview persons of a specified description who process personal data on behalf of the data controller.

The ICO's Regulatory Action Policy sets out that it will issue an assessment notice in the following circumstances:

- When a **risk assessment or other regulatory action determines there is a probability that personal data is not being processed in compliance** with the data protection legislation, together with a likelihood of **damage or distress** to individuals;
- When it is necessary to verify **compliance with an enforcement notice;**
- When communications with the controller or processor, or information about them (e.g. news reports, statutory reporting or publications) **suggests that they are not processing personal data in compliance** with the data protection legislation;
- The controller or processor has **failed to respond to an information notice** within an appropriate time.

When determining if there is a risk of non-compliance, the ICO will consider one or more of the factors for regulatory action set out in the Regulatory Action Policy. They will also consider other relevant information, such as reports by whistle-blowers, and any data protection impact assessments that may have been carried out.

[6] Provisions for assessment notices are set out in Sections 146-148 of the DPA 2018, including restrictions to this power.

Sometimes, the ICO may need to issue an **urgent assessment notice**. This may require access to non-domestic premises with less than seven days' notice. In the most serious cases, the notice may allow the ICO to carry out a **no-notice inspection**. To decide the period of compliance with assessment notices, the ICO will use the same criteria outlined above for information notices.

Assessment notices **may be enforced by the ICO obtaining a warrant** and exercising search and seizure powers. Conditions for these are set out in Schedule 15 to the DPA 2018. It is an offence under paragraph 15 of that Schedule to obstruct a warrant.

It is also an **offence** under the DPA 2018 to destroy or falsify information and documents or similar material once a person has been given an information notice or assessment notice[7]. This offence acts as a deterrent against a person taking such steps to try to prevent the ICO from having access to information or documents.

Enforcement Notices

The ICO can issue an enforcement notice if it determines that specific corrective action is required.[8] An enforcement notice will include what its recipient has failed or is failing to do; why the ICO have reached that opinion; and the actions the recipient must take or refrain from taking (e.g. must not continue processing).

The purpose of such a notice is to remedy compliance failures. The types of failures that can be the subject of an enforcement notice are set out in Section 149(2-5). The ICO's Regulatory Action Policy sets out a non-exhaustive list of circumstances where they may issue an enforcement notice:

- **Repeated failure** to meet data protection obligations or timescales for them (e.g. repeatedly delayed subject access requests);
- Where **processing or transfer of information to a third country fails** (or risks failing) to meet the requirements of the data protection legislation;
- Where there is an **ongoing NIS incident** requiring action by a digital service provider there is a need for the ICO to require communication of a data security breach to those who have been affected by it[9]; or
- There is a **need for corrective action** by a certification body or monitoring body to ensure that they meet their obligations.

The deadlines in an enforcement notice will usually reflect:

[7] Section 148 of the DPA 2018.
[8] Sections 149-153 set out provisions for enforcement notices, including restrictions on this power.
[9] NIS stands for the 'Network and Information Systems Regulations 2018', implementing the European Directive 2016/1148 on a high common level of security of network and information systems across the Union.

- The imminence of proposed action that could lead to a breach of obligations;
- The severity and scale of any breach/failings; and
- The feasibility (including lead times) of any correcting measures or technology.

Sometimes the ICO may need to issue "urgent" enforcement notices. In such a case, the ICO must still allow at least 24 hours for the recipient to comply. The ICO will consider a number of factors when deciding whether it is proportionate to issue an urgent notice, and the length of the period. These factors are set out in its Regulatory Action Policy and include:

- The extent to which such urgent action may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy. For example, requesting a data controller stops using personal data for a specific purpose or takes action to protect personal data from security breaches;
- The scope of the enforcement notice;
- The additional burden or impact on the recipient in having to comply with an urgent enforcement notice within the period specified; and
- The comparative effectiveness of other enforcement powers of the ICO.

If a data controller or data processor fails to comply with an enforcement notice, the Commissioner will also consider whether or not to issue a Penalty Notice.

Penalty Notices

Penalty notices[10], i.e. fines, may be necessary to ensure compliance with data protection legislation. The ICO may issue such a notice when:

- There has been a compliance failure set out under Section 149 (2), (3), (4), or (5); or
- A person has failed to comply with an information notice, an assessment notice, or an enforcement notice.

How the ICO decides whether to impose a penalty notice

Article 83 of the UK GDPR sets out various factors to take into account when deciding whether to impose a fine. The ICO emphasises the below factors in its Regulatory Action Policy:

- **The scope of the breach**:
    - Its nature, gravity, and duration;
    - The categories of personal data affected by the failure;
    - The number of affected individuals.
- **The behaviour of the controller of processor**:
    - Whether the breach was intentional;
    - How the infringement became known to the ICO, including whether, and to what extent, the controller or processor notified the ICO of it;

[10] Provisions for penalty notices are set down in sections 155-159 of the DPA 2018, including restrictions on these powers.

  - Any mitigating action taken by the organisation;
  - The degree of cooperation with the ICO investigation to remedy the failure and mitigate its risks;
  - The extent to which the data controller or data processor has complied with previous enforcement notices or penalty notices;
  - Tny history of previous failures;
  - Adherence to approved codes of conduct or certification mechanisms.
- **Other key factors:**
  - Whether the penalty would be effective, proportionate and dissuasive;
  - Any other relevant aggravating or mitigating factor, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly).

The Policy notes that a penalty is a more likely outcome in cases when it involves:

- A number of affected individuals;
- A degree of damage or harm (which may include distress and/or embarrassment);
- Sensitive personal data;
- A repeated breach of obligations or a failure to fix a previously identified problem or follow previous recommendations;
- Wilful action or inaction;
- A failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it); and
- A failure to implement the accountability provisions of the GDPR.

How the ICO decides the amount of the penalty notice

If the ICO has decided to issue a penalty notice, the factors listed above are also relevant for **setting the amount**. The Regulatory Action Policy emphasises five components of the ICO's approach to the amount:

1. The need to remove any financial gain from the breach;
2. The need to censure the breach based on its scale and severity;
3. The need to reflect any aggravating factors;
4. The need to deter other potential violators;
5. The need to reflect any mitigating factors, but not to the extent any reduction in the amount still permits financial gain from the breach;

In keeping with all the factors outlined above, the Policy notes that the amount of the penalty **will tend to be higher** in cases where:

- Vulnerable individuals or critical national infrastructure are affected;
- There has been deliberate action for financial or personal gain;
- Advice, guidance, recommendations, or warnings (including those from a data protection officer or the ICO) have been ignored or not acted upon;
- There has been a high degree of intrusion into the privacy of a data subject;

- There has been a failure to cooperate with an ICO investigation or enforcement notice; and
- There is a pattern of poor regulatory history by the target of the investigation.

Maxima for the fines are set out in Article 83 of the UK GDPR and section 157 of the DPA 2018, depending on the nature of the breach. The highest possible fine is £17.5 million or 4% of an undertaking's annual global turnover, whichever is higher.

Steps before issuing any penalty notice

Before issuing a penalty, the ICO issue a **Notice Of Intent (NOI)**[11], setting out the breach's circumstances, the investigation findings, the proposed penalty, its rationale, and any proposed enforcement notice requirements.

The NOI allows recipients the opportunity to make representations about the ICO's intention to issue a penalty, within a specified time period of at least 21 calendar days. No penalty may be given before the end of that period.

The ICO must consider any representations made when deciding whether to give a penalty notice, and determining the amount. When the ICO intends to issue a very significant penalty, i.e. over £1m, it may convene a Regulatory Panel of three senior people, independent of the investigation to consider the case and representations made. It will make a recommendation, but the Commissioner retains the final decision.

After fully considering all representations, the ICO will confirm any penalty notice in writing.

Appealing ICO Enforcement Action

Appeals to information notices, assessment notices, and enforcement notices

If a person has received one of the above notices, they may appeal the notice to the First Tier Tribunal within 28 days. Where the notice is **not an urgent notice**, a person cannot be required to comply with the notice until the time period for bringing an appeal is over. If the recipient does indeed appeal, compliance is not required until and unless the appeal has failed or been withdrawn[12].

A recipient of an **urgent** information notice, assessment notice, or enforcement notice may apply to court to overturn the urgency of that notice or to vary the time period for compliance, for all or some of its requirements.

[11] Schedule 16 to the DPA 2018.
[12] Section 142(5) and (6); Section 146(6) and (7); Section 150(6) and (7); and Section 162.

Appeals to penalty notices

A recipient of a penalty notice may also appeal this to the Tribunal within 28 days. They may appeal either the notice itself, or the amount, or both[13].

Beyond the First Tier Tribunal

Appeals to any of the above notices that raise particularly complex or important issues may be transferred to the Upper Tribunal.[14] The Upper Tribunal also hears appeals against decisions of the First Tier Tribunal.

Where a person is dissatisfied with a decision of the Upper Tribunal, they may seek permission to appeal to the relevant appellate court. This may be the Court of Appeal in England and Wales, the Court of Session in Scotland, or the Court of Appeal in Northern Ireland.

Criminal offences

The DPA 2018 also gives the ICO the power to prosecute those who commit criminal offences under the Act or refer cases to the appropriate prosecutor. Criminal offences under the Act[15] include those around:

- Providing false statements in response to an information notice;
- Deliberately destroying or concealing evidence identified as being relevant to an investigation;
- Unlawfully obtaining, disclosing, or retaining personal data without the consent of the controller;
- Re-identification of de-identified personal data;
- Altering, concealing, etc, personal data to prevent disclosure to the data subject; and
- Forcing certain employees or contractors to produce certain records as a condition of their employment or contract.

Criminal prosecution penalties are determined by the courts and not by the ICO.

Recent enforcement activity

Responding to cyber security incidents

The ICO works closely with key strategic partners, including the UK's National Cyber Security Centre in supporting its goal to provide a unified national response to cyber threats. In recognition of the growing threat profile of cyber incidents and the risks they pose to consumers and data subjects, the ICO has created a dedicated team to investigate and

[13] Section 162

[14] Any case considering data protection and national security must be transferred to the UT (Rule 19 of SI 2009/1976). This is covered in more detail in Sections F and H.

[15] Sections 119; 132; 144; 148; 170; 171; 173; 184; and Schedule 15.

where appropriate, take action, in response to data protection infringements which result in significant data breaches.

Civil enforcement

The ICO publishes details of the regulatory action it takes against data controllers and data processors on its website.[16] Some recent cases include:

- In July 2019, the ICO issued a Notice of Intent to fine **British Airways £183.39 million**, and a Notice of Intent to fine **Marriott International, Inc £99.2 million;**
- In 2018, the ICO issued the maximum fine **under the DPA 1998 - £500k - to Equifax for failure to adequately protect systems** containing large volumes of consumer data. Approximately 146 million people were affected globally, including 15 million UK users. The company had previously been notified that there were deficiencies in their arrangements by the US Department of Homeland Security;
- In 2018, **the Crown Prosecution Service (CPS) was fined £325,000** by the ICO after they lost unencrypted DVDs containing recordings of police interviews;
- In 2018, **The Carphone Warehouse Ltd was fined £400,000** after serious failures placed customer and employee data at risk;
- In 2018, **Humberside Police was fined £130,000** by the ICO after disks containing a video interview of an alleged rape victim went missing;
- In 2018, **The University of Greenwich was fined £120,000 by the Information Commissioner**, following a "serious" security breach involving the personal data of nearly 20,000 people. Some of this data was sensitive, such as information on extenuating circumstances, details of learning difficulties, and staff sickness records, and was subsequently posted online.

The ICO has also actively participated in European Data Protection Board Taskforces for coordinated enforcement. In 2018, the ICO fined Uber £385,000. Action was taken against the Netherlands based Uber BV and 4 affiliate UK based companies. 2.7 million UK users were affected by Uber's data breach. This was a complex case with international cross-jurisdiction impact, which required ICO involvement in an EDPB Taskforce, and engagement with Transport for London, other regulatory agencies, and Government departments.

Furthermore, in May 2017 the Commissioner launched an investigation into the use of data analytics for political purposes known as *Operation Cederberg*. This followed concerns about invisible processing: the 'behind the scenes' algorithms, analysis, data matching and profiling that involves people's personal information. The ICO also took a leading role in enforcement of the breach of Facebook user's data protection by Cambridge Analytica.

[16] This can be found at https://ico.org.uk/action-weve-taken/enforcement/.

Section G: Role of the ICO and Redress

During the course of the investigation, which remains ongoing, the Commissioner has used her powers to improve compliance by political parties, referendum campaigns, social media organisations and data analytic companies by using the range of powers available to her.

These have included information notices, enforcement notices, civil monetary penalties, search warrants and audits. SCL Elections Ltd was prosecuted for failing to comply with an enforcement notice recently resulted in a guilty plea by the organisation and a £15,000 fine with £6,000 costs.[17]

Criminal enforcement actions

- In 2018/19, the ICO made a decision to prosecute 17 cases in relation to data protection offences including the **unlawful obtaining or disclosure of personal data** and administered 10 cautions;
- In 2017/18, the ICO prosecuted 19 cases in relation to the **unlawful obtaining or disclosure of personal data** under Section 55 of the DPA 1998. The ICO issued a further 6 cautions;
- In 2018/19, the court imposed the highest fine for breaches of Section 55 of the DPA 2018 in relation to the investigation into the **unlawful obtaining of personal data by private investigators on behalf of corporate clients**. A high-profile and landmark prosecution following the ICO's investigation supported by the NCA, resulted in the prosecution of the company, a director, a senior employee and 2 private investigators;
- 2018/19 also saw the first prosecution by the ICO for an offence contrary to Section 1 of the Computer Misuse Act 1990 (CMA 1990), an offence which has a maximum sentence of imprisonment. The decision was taken to prosecute under the CMA due to the nature and extent of the offending by the Defendant. The sentence given was six months imprisonment[18].

[17] The ICO's aggregated report including enforcement action can be found at: https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/. A press release was published at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/scl-elections-prosecuted-for-failing-to-comply-with-enforcement-notice/.

[18] Six month prison sentence for motor industry employee in first ICO Computer Misuse Act prosecution.

PART III: GOVERNANCE AND INDEPENDENCE OF THE ICO

This part outlines key elements of the ICO's set-up and governance. It sets out the requirement for its independence; its relationship with Government and Parliament; how the Commissioner is appointed; and various other governance matters such as funding, spending controls, and staffing.

Independence and Accountability for Performance

Independence is at the core of the ICO's set up. Article 52 of the UK GDPR requires that the ICO:

- Shall **act with complete independence** in performing its tasks and exercising its powers in accordance with the UK GDPR;
- Remain **free from external influence, whether direct or indirect**, in relation to those tasks and powers; and
- Shall **neither seek nor take instructions** from anyone.

The ICO sets its own priorities and has independently set its own Information Rights Strategic Plan, and associated strategies and plans[19].

The ICO **is directly accountable to Parliament** and reports against agreed key performance indicators to a Select Committee. The ICO produces an Annual Report to Parliament, which is not signed, reviewed or agreed by Government.[20]

It is not held to account by any department or Ministry, and the Government has no right of review or alteration over regulatory decisions.

The ICO's independence was particularly demonstrated when it issued a fine to its then sponsor department in 2014. The ICO fined the Ministry of Justice £180,000 for the loss of an unencrypted backup hard drive containing personal data on 2,935 prisoners.

The Constitution of the ICO's Office

The Information Commissioner is a "Corporation Sole": a separate legal entity constituted in a single person. All powers and responsibilities are vested in the Commissioner.

In particular, the Commissioner is:

- The regulatory decision maker, responsible for the exercising of the powers and tasks outlined in Chapter VI of the UK GDPR;
- The Accounting Officer, responsible for finances, spending, budgeting and internal controls; and

[19] https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/.
[20] Section 139 of the DPA.

- Chief Executive, responsible for managing the organisation, setting strategic direction, and delivering performance.

The Commissioner has delegated many responsibilities to individuals within the ICO through a formal delegation scheme.

The ICO's **Management Board** is responsible for assisting the Information Commissioner in discharging their statutory responsibilities at a strategic level. The Board consists of Non-Executive Directors and Executive Directors. They are appointed by the Commissioner, with **no input from the Government or Parliament**.

The Commissioner also has responsibility for appointing deputy commissioners. Their responsibility for appointing other staff is outlined further below. The Government has no involvement in the appointment or promotion of ICO officials.

Appointment and removal of the Information Commissioner

Appointment of the Information Commissioner

The terms of appointment of the Information Commissioner are set out in Schedule 12 to the Data Protection Act 2018. Following a thorough, independent, transparent selection and appointment process, the Commissioner is appointed by Her Majesty the Queen, upon a recommendation from Government.

No recommendation may be made to Her Majesty for the appointment of a person as the Commissioner **unless the person concerned has been selected on merit on the basis of fair and open competition**. The Secretary of State's recommendation is primarily based on the decision of an independent panel. When making the recommendation, the Secretary of State should consider the advice of Advisory Assessment Panels. The recommendation is subject to public scrutiny by Parliament in the form of a hearing by the DCMS Select Committee[21].

The appointment of the Information Commissioner, and other DCMS public appointments, are regulated by the Commissioner for Public Appointments in line with the Cabinet Office Governance Code on Public Appointments[22].

Term duration and removal

The Commissioner is to hold office for a non-renewable term not exceeding 7 years.[23] **No Minister, Prime Minister, or civil servant can remove the Commissioner**. They can only be

[21] Transcript of the pre-appointment hearing of Elizabeth Denham (27 April 2016)
[22] Cabinet Office Governance of Public Appointments (published December 2016):
[23] Paragraphs 2(3) to (4) of Schedule 12 to the DPA 2018

removed by Her Majesty following an agreement by both Houses of Parliament**.** Parliament will only consider removal if a Minister presents a report stating they are satisfied that:

- The Commissioner is guilty of gross misconduct; or
- The Commissioner no longer fulfils the conditions required for performing their functions .

Her Majesty may also relieve the Commissioner of their office at their own request. [24]

DCMS's sponsorship of the ICO

The ICO has a 'sponsorship' relationship with the DCMS. This allows the ICO to access DCMS's resources, expertise, and networks.

The relationship is governed by a publically available Management Agreement[25]. The key responsibilities of a sponsoring department include:

- Ensuring that the ICO is adequately funded and resourced;
- Representing the interests of the ICO to Parliament and other Government departments;
- Ensuring that there is a robust national data protection framework in place;
- Providing guidance and support to the ICO on corporate issues such as estate issues, leases and procurement.

The Agreement exists to set out the differing roles and responsibilities of the Department and the ICO. It was developed in line with the requirement that the ICO be completely independent, remain free from any external influence, and neither seek nor take instructions when performing their tasks as a supervisory authority.

Funding and Spending

Funding

The ICO is financed through the retention of data protection charges collected from data controllers under the Data Protection (Charges and Information) Regulations 2018.

The funding model **safeguards the ICO's statutory independence** by ensuring an adequate and stable level of funding, with no recourse to public funds in respect of the ICO's data protection functions.[26]

[24] Paragraph 3 of Schedule 12 to the DPA 2018 sets out conditions for resignation and removal.
[25] Management Agreement 2018-2021.
[26] The ICO does receive government funding and grant-in-aid for certain of their other functions, including work related to FOIA, eIDAS as mentioned earlier in this section.

The charge levels have been increased from the previous level of fees to reflect the increased responsibilities of the ICO under the DPA 2018. A financial forecast for the first year of operation under the DPA 2018 (2018/19) set the income requirement for the ICO at approximately £30 million (34€ million).[27]

If a controller fails to pay a data protection fee under the above Regulations, the ICO has the power to issue fixed penalties.[28] These are set according to the size of the controller's organisation. They are different from penalties for failure to comply with data protection requirements, which are instead subject to a statutory maximum and outlined in Part III of this section. Any monetary penalty is paid into the Treasury's Consolidated Fund and is not kept by the ICO.

Spending

The Commissioner is also the ICO's Accounting Officer: responsible for the office's budget and accountable for how money is spent. They are also the ICO's Chief Executive Officer and so responsible for decisions on the office's resourcing and organisation.[29]

As with all public sector organisations, the ICO is subject to the latest Cabinet Office spend controls[30]. It is also subject to the DCMS thresholds for spend controls, set out in the latest DCMS Spend Control Guidance. The Management Agreement sets out that there is an exception to processes set out in the Guidance for advertising and marketing campaigns under £100,000. For such expenditures, the ICO need only request approval from the DCMS Sponsorship Team.

Staffing

DCMS has no involvement in the appointment or promotion of ICO officials. The Commissioner has statutory responsibility for the appointment of officers and staff, as well as for determining their pay and conditions of service.[31] The Management Agreement outlines that the Commissioner *"should ensure that arrangements are conducive to the recruitment and retention of the staff needed to enable them to fulfil their statutory duties. Pay and conditions are expected to be affordable, proportionate and responsible, including senior salaries".*

In January 2018, it was decided that the ICO should have pay flexibility up to 2020/21 to ensure it can review its pay and grading structure. The ICO has to submit an annual pay remit to DCMS for approval. However, during the specified three year period of pay flexibility, this will be for information purposes only.

---

[27] The final outturn for the financial year was £39 million.
[28] Section 158 of the DPA 2018.
[29] Paragraph 5 and 11 of Schedule 12 to the DPA 2018.
[30] Cabinet Office Spend Controls
[31] Paragraph 5 of Schedule 12 to the DPA 2018.

PART IV: GUIDANCE AND ADVICE

This part highlights various elements of the ICO's activities in providing guidance to organisations and sectors, and advice to organisations, fellow regulators, and Government.

Guidance

Preparing for GDPR

During the GDPR implementation phase up, the ICO:

- Launched a **dedicated helpline service for smaller organisations**;
- **Updated its 'SMEs toolkit'** to reflect the requirements of the GDPR;
- Published **"12-step" GDPR preparation** guidance; and
- **Developed FAQs** for a range of organisations and sectors.

During this period, the ICO also delivered an awareness-raising marketing campaign targeted at those organisations and sectors, including SMEs, which were most in need of support.

Whilst a member of the European Data Protection Board, the ICO led the development of key European guidelines such as those addressing:

- The definition of lead supervisory authority;
- Breach reporting obligations;
- Profiling and automated decision-making; and
- Calculation of fines.

It also co-led work on guidelines addressing consent, codes of conduct, certification, and transparency. This work has been fed into the ICO's comprehensive suite of information rights guidance, which is internationally recognised **for its clear and practical approach**.

Today, the ICO has a comprehensive Guide to Data Protection[32] that addresses GDPR and the domestic modifications made to it by the DPA 2018. It also covers the DPA 2018 provisions implementing the Law Enforcement Directive and will be expanded soon to cover intelligence service processing.

The Guide has had in excess of 16 million unique views and explains to data controllers and data processors what they need to do to comply with data protection law. It is a key source that ICO staff refer to when undertaking their regulatory duties and is used in the context of appeals and court interventions.

[32] https://ico.org.uk/for-organisations/guide-to-data-protection/.

Section G: Role of the ICO and Redress

The ICO has developed a range of complementary tools and resources to further assist controllers and processors to understand their legal duties. This includes interactive tools to work through how the lawful bases for processing work, Data Protection Impact Assessments (DPIA) and privacy notice templates and podcasts to discuss key issues.

Further work on guidance for controllers

The ICO is developing several statutory codes of practice that it is required to produce under the DPA 2018. These address data sharing, journalism, direct marketing and age appropriate design for information society services likely to be accessed by children. These codes explain how organisations can comply with data protection requirements.

The age appropriate design code is world-leading in defining how information society services should take a privacy by design approach that is appropriate to the needs of child users. This is a practical measure to make the GDPR provisions which acknowledge that children deserve special protection a reality.

The ICO continues to develop guidance related to specific types of processing where its investigations identify a need for greater clarity for data controllers. Following the publication of its '*Democracy Disrupted?*' report, the ICO has published a draft code of practice for the use of personal data in political campaigning.[33] The ICO has also been investigating the use of live facial recognition technology.[34] The findings from its report could lead to an update of its code of practice on the use of surveillance technologies.[35]

Guidance on Artificial Intelligence

The ICO has won awards for its work including for its paper on big data and AI which won the 'people's choice' award at the 2017 International Conference of Data Protection and Privacy Commissioners as voted for by other DPAs. Building on this success, the ICO appointed a Postdoctoral Research Fellow to lead its work on researching and developing a framework for auditing algorithms, as well as conducting further in-depth research into AI and machine learning.[36]

This work is considering, amongst other aspects, the explainability of automated-decisions to data subjects, the role of meaningful human reviews, the accuracy of AI system outputs, and security risks which could be exacerbated by the use of AI. The ICO expects to publish a consultation paper on its AI accountability framework in early 2020.

Guidance to data subjects

[33] https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf.
[34] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/.
[35] https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf.
[36] https://ai-auditingframework.blogspot.com/

Section G: Role of the ICO and Redress

The ICO also produces clear advice and guidance to individuals to help them understand what their rights are with regards to their personal data as part of its 'Your Data Matters' section of the ICO website.[37] This includes guidance on each of the data protection rights in respect of controllers, as well as the right to make a complaint to the ICO. There is also guidance on more specific topics such as credit reference files, identity theft, and the use of CCTV systems in domestic settings.

When the ICO develops its guidance, it will often develop complementary resources for data subjects alongside drafting guidance for controllers. This has already been done for political campaigning practices and charity fundraising practices.

In addition, the ICO has launched a 'Be Data Aware' campaign to help the public understand more about how companies use personal data and what individuals can do to increase their own privacy online.

Providing Advice

Regulatory sandbox[38]

The first round of the sandbox will proactively support ten organisations across the private and public sectors to develop innovative products and/or services that make use of personal data and that benefit the public.

The beta phase will run from July 2019 until September 2020 and is particularly focused on achieving both compliance and supporting these developments coming to fruition. The aim is therefore to avoid potential issues from becoming problems which require investigation and enforcement at a later stage in their development.

The ICO will be seeking to provide this support to innovations at their design, proof of concept, and testing stages, or as further ongoing development of existing innovative products/services. **No requirements for compliance with the UK GDPR or DPA 2018 will be relaxed through this process**.

The sandbox will play a crucial role in ensuring that the ICO keeps pace with technological changes and the way that personal data is used. For example, through the service, the ICO's guidance will continue to be informed by the real practical experiences of the challenges faced in monitoring compliance in innovative contexts, ultimately improving its effectiveness in helping controllers achieve compliance.

[37] https://ico.org.uk/your-data-matters/

[38] Further information can be found in the ICO's Guide to the Sandbox at https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/

Section G: Role of the ICO and Redress

Regulators' Business Innovation Privacy Hub

In December 2018, the ICO's Regulators' Business Innovation Privacy Hub (The Hub) was created, with funding from the Department for Business, Energy and Industrial Strategy (BEIS).

Its aim is to help businesses embed data protection by design and have the confidence to create innovative products and services that are effective, compliant, and build customer trust in how their data is used.

The Hub will collaborate with a number of regulators through their own sectoral Sandboxes, including the Financial Conduct Authority, Civil Aviation Authority, Care Quality Commission and the Solicitors Regulatory Authority. The Hub has also supported other regulatory activity to support business innovation and ensure greater reach of data protection awareness. Activities so far include:

- The provision of advice to the Medicines and Healthcare products Regulatory Agency regarding the development and use of synthetic data; and
- Advisory support to participants of the Financial Conduct Authority's TechSprint on privacy-enhancing technologies.

The Hub is exploring other opportunities for collaboration including:

- Provision of advice to regulators via relevant working and advisory groups;
- Working with Catapult and other Innovation centres in the UK; and
- Supporting other organisations and bodies developing their own sandbox models.

The ICO intends to continue operating the Hub after BEIS funding ends in April 2020. Although its activities will move outside the project scope as it currently stands, it is likely that the core principles of cross-regulatory collaboration and information sharing will play a key role moving forward.

Data protection impact assessments

The ICO created a new Data Protection Impact Assessment (DPIA) Team in May 2018 in order to fulfil the Commissioner's obligations under Article 36 of UK GDPR and Section 65 of the Data Protection Act 2018 (prior consultation). The Commissioner is required to provide advice within statutory timescales in cases where DPIAs for new projects identify residual high risk to data subjects.

The ICO issued a list of general processing operations which it considers are likely to result in a high risk, and therefore require a DPIA to be completed prior to commencement.[39] This list

[39] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/.

was revised in light of opinion 22/2018[40] of the European Data Protection Board, with a final version published in the ICO's revised DPIA guidance in late 2018.

In the first fifteen months following 25 May 2018, the ICO received 33 requests for prior consultation from controllers. In some cases, prior consultation has led to warnings being issued as, in the opinion of the Commissioner, the proposed processing operations as described by the controller would contravene data protection law.

Legislative consultations

The Commissioner is tasked by Article 57(1)(c) of the UK GDPR with advising the UK Parliament and the UK Government, as well as other institutions, on legislative and administrative measures relating to data protection.

The DCMS has published guidance for Government departments[41], including the devolved administrations in Scotland, Wales and Northern Ireland, to consult the ICO on proposals for new legislative or regulatory measures which would involve the processing of personal data as per Article 36(4) of the UK GDPR.

The ICO also regularly gives written and oral evidence to the UK's legislatures. In recent years this has included giving evidence to:

- The House of Commons' Digital, Culture, Media and Sport Committee's inquiry into disinformation and 'fake news'[42], including appearing before the 'international grand committee' composed of elected representatives from seven national legislatures;
- The House of Lords' Communications Committee's inquiry into internet regulation[43];
- The Joint Committee on Human Rights' inquiry into the right to privacy and the digital revolution[44]; and
- The Scottish Parliament's Justice Sub-Committee on Policing's inquiry into Police Scotland's Digital, Data and ICT strategy (digital device triage systems).[45]

Codes of Conduct and Certification

The ICO is encouraging the adoption of codes of conduct and certification by controllers and data processors as key voluntary accountability tools. They are important new co-regulatory

[40] https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222018-united-kingdom-sas-dpia-list_en.
[41] https://www.gov.uk/government/publications/guidance-on-the-application-of-article-364-of-the-general-data-protection-regulation-gdpr.
[42] https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/.
[43] https://www.parliament.uk/business/committees/committees-a-z/lords-select/communications-committee/inquiries/parliament-2017/the-internet-to-regulate-or-not-to-regulate/.
[44] https://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/inquiries/parliament-2017/right-to-privacy-digital-revolution-inquiry-17-19/.
[45] https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/108429.aspx.

tools that will further support the ICO's wider regulatory function and could be the basis for international transfers of personal data in certain sectors.

The ICO contributed to the drafting of the EDPB guidelines as a member of the Board and assisted in the designing and trialling of the EDPB's certification and accreditation approval procedures. It intends to apply that approach to codes of conduct and certification schemes in the UK.

The certification schemes will be strengthened by the use of the UK Accreditation Service (as the UK's national accreditation body) to accredit the certification bodies. This will be piloted once the first certification scheme has been submitted.

PART V: INTERNATIONAL ROLE AND ACTIVITIES

This part sets out the ICO's international duties, and its activities in various international regulatory fora and groups. As well as developing working relationships with international colleagues, the ICO's work with these groups helps to **ensure that UK data protection law and practice is a benchmark for high global standards.**

The ICO's International tasks

The ICO is the designated authority in the UK for the purposes of the Council of Europe's Convention for the Protection of Individuals with Regard to the Processing of Personal Data ("**Convention 108"**). Its tasks under Convention 108 include cooperating with other signatories' authorities, such as sharing information and providing mutual assistance.

Beyond the Data Protection Convention, the Commissioner has further duties to develop cooperation mechanisms, provide mutual assistance, engage relevant stakeholders and promote the exchange of good practice in data protection with any third country or international organisation.

The Commissioner also has a power to inspect personal data where necessary to discharge an international obligation of the United Kingdom.[46] This could include inspecting the processing activities of a controller in the UK in a database used for exchanging information between several countries, to ensure it complies with the data protection provisions governing the use of that database. In the past, this power has been used to conduct audits of the UK's SIRENE Bureau for the Schengen Information System.

The Commissioner published an International Strategy for 2017-2021.[47] The strategy outlines the four key challenges in the ICO's international work in that period and the priorities for meeting those challenges.

International activities

The ICO is highly respected by fellow regulators around the world, and made a significant contribution to the work of the European Data Protection Board as a member. Many EU regulators have re-used the ICO's domestic guidance and the ICO contributes to the EU's world-leading expertise and global influence.

The ICO has taken a prominent role in a number of international networks. This includes involvement with:

- The **Global Privacy Assembly** (GPA), previously known as the **International Conference of Data Protection and Privacy Commissioners** (ICDPPC). This brings

[46] Section 119 of the DPA.

[47] https://ico.org.uk/media/about-the-ico/documents/2014356/international-strategy-03.pdf.

together around 120 data protection authorities across the world. In October 2018, the Commissioner was elected as chair of ICDPPC, giving the UK an ability to not just share policy and enforcement experience but to take on a leadership role within the global privacy and information rights community;

- The **Global Cross Border Enforcement Cooperation Arrangement** as endorsed by the ICDPPC in 2017;[48]
- The **Asia Pacific Privacy Authorities (APPA)**, where the ICO attended forum meetings in December 2018 and May 2019. The Commissioner spoke at the forum meeting in New Zealand, on regulatory convergence and international collaboration. Following attendance at the APPA event in Japan in May 2019, the Commissioner delivered the closing keynote speech at a G20 side event on the topic of "International seminar on personal data";
- **The Common Thread Network (CTN)**, which the ICO co-chairs with the Ghana Data Protection Commission. This brings together data protection and privacy regulators across commonwealth countries. The ICO hosted an event on privacy, trust and the digital economy in the Commonwealth in April 2018 and represented the CTN at the first African Regional Data Protection Privacy Conference in June 2019 in Accra. This will give it the opportunity to promote data protection and privacy laws in Africa;[49]
- **The Global Privacy Enforcement Network (GPEN),** which aims to increase cooperation in the enforcement of privacy laws across borders;
- **The Unsolicited Communications Enforcement Network (UCENet)** which brings together a range of regulators with a common interest in preventing and taking enforcement action against those transmitting unsolicited communications.

Bilateral cooperation with other countries' authorities

The ICO has also worked closely with the USA's Federal Trade Commission (FTC), giving evidence on international cooperation, competition, privacy, and GDPR. It has also been working with the FTC to share expertise to assist in the expansion of their data protection capacity and capability.

The ICO also worked with the Foreign and Commonwealth Office to inform the introduction of Brazil's data protection law. This included speaking at events in Brazil in April 2019.

Cooperation through information sharing and Memoranda of Understanding

As a member of the EDPB, the ICO has been an active participant in the Internal Market Information (IMI) System – a secure, multilingual online information exchange tool. Since the introduction of the GDPR, this has been used to cooperate with other supervisory authorities in the EU in order to facilitate the handling of investigations.

[48] https://globalprivacyassembly.org/
[49] https://www.commonthreadnetwork.org/

Section G: Role of the ICO and Redress

Within the first year of the introduction of GDPR, the ICO was involved in close to **150 investigations** from other supervisory authorities in the EU, as well as **referring roughly 100 cases** to other supervisory authorities though the cooperation procedure. In addition, the ICO responded to 10 mutual assistance requests and sought 2 opinions from the EDPB.

In addition, the ICO has developed **international memoranda of understanding.** These cover information sharing for enforcement purposes, tactical exchanges of information, and intelligence sharing.

The ICO has supported a myriad of investigations by other data protection authorities and received information in turn from other authorities to assist its regulatory work, not least in the investigations into the use of personal data analytics for political campaigning.

PART VI: REMEDIES AND REDRESS

Data subjects with concerns about information rights practices can pursue various remedies to enforce their rights rapidly and effectively, and ensure compliance.

This can take the form of complaints to the ICO, including via their website form. During 2018/19, the ICO saw the number of complaints received from data subjects almost double with 41,661 complaints compared to 21,019 in 2017/18.[50]

Complaints may result in the enforcement actions outlined earlier in Part 2, including penalties. Alternatively, data subjects may seek a **judicial** remedy. This provides for a system of independent adjudication, which allows compensation to be paid and sanctions imposed where appropriate.

Data subjects may seek a judicial remedy from the start, or they may proceed to court after having already complained to the ICO. They may also in some instances seek a judicial remedy against the ICO or lodge a complaint in relation to its service.

This part sets out the various remedies there are. It covers:

- Data subjects' ability to go to court for redress against controllers or processors, including for compensation claims;
- Data subjects' remedies in case of dissatisfaction with ICO service.

Data subjects' ability to seek judicial redress against controllers or processors

Bringing controllers or processors into compliance

Article 79 of the UK GDPR sets out that data subjects have a right to seek a judicial remedy against a controller or processor. Section 167 of the DPA 2018 empowers courts to make an order for compliance, requiring controllers to take or refrain from taking specific steps where a data subject's rights, under data protection legislation, have been infringed.

Compensation

Article 82 of the UK GDPR gives data subjects the right to claim compensation for financial losses and other damage suffered as a result of infringement of the UK GDPR. Some solicitors will take cases on a "no win no fee" basis if the case has good prospects.[51]

[50] The ICO has details of the complaints received and closed, as well as the nature of the complaint in their annual report. This can be found at: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

[51] Further information can be found at: https://ico.org.uk/your-data-matters/data-protection-and-journalism/taking-your-case-to-court-and-claiming-compensation/.

Section 168 of the DPA 2018 makes clear that this includes a right to claim damages for distress. Section 169 of the DPA 2018 further provides the right to compensation for the contravention of other data protection legislation.[52]

The DPA 2018 is the primary legislation relied upon to bring data protection breach compensation claims, but other laws a claimant may rely on for compensation include the:

- Privacy and Electronic Communications (EC Directive) Regulations 2003;
- Human Rights Act 1998.

Each right of action has its own **time limit** by which a claimant must have issued proceedings in court. For example, (subject to exceptions) claimants have one year to issue proceedings under the Human Rights Act, but **six years** to issue proceedings under the DPA 2018.

There is no **set amount of compensation** for a breach of the Data Protection Act. The level of award is determined by the courts and varies depending on the extent of damage and/or distress caused. Compensation claims may be composed of general damages and special damages. General damages are not easily quantified and include things like emotional damage, distress, and loss of future employment prospects. Special damages can be valued financially, such as lost earnings and travel expenses.

Collective actions

Provisions for collective action (i.e. by more than one claimant) vary depending on the jurisdiction. Under the Civil Procedure Rules for England and Wales, collective action may take place via group litigation orders, or a representative action.

Data subjects' remedies in case of dissatisfaction with ICO service

Judicial remedies against the ICO

The right to an effective judicial remedy against a legally binding decision of the ICO is set out under Article 78(1) of the UK GDPR. A data subject can apply to the High Court, or the Court of Session in Scotland, for a **Judicial Review** where the complaints process has been exhausted.

Judicial review is a process which is used to challenge decisions made by public bodies, where the court reviews the lawfulness of a public body's decision. Grounds for judicial review include unreasonableness, illegality, procedural unfairness, legitimate expectation, and human rights breaches.

[52] An example of a data protection compensation claim: the County Court awarded a former police officer £9,000 in damages for breaches after her personal information was improperly accessed by police forces. (Brown v Commissioner of Police of the Metropolis and Chief Constable of Greater Manchester Police, Claim Nos 3YM 09078 and A53YP250, 7 October 2016.)

If the court decides that the ICO has acted unlawfully, it may provide a remedy such as:

- Quashing the decision and requiring the body to retake the decision;
- Requiring the body to take some other step or to not take certain action;
- Making a declaration; and/or
- Awarding damages (in limited circumstances).

As outlined above, data subjects may also proceed to take the controller or processor to court for the matter under Article 79 of the UK GDPR and Section 167 of the DPA 2018, and the court may take a differing view from any ICO decision.

Article 78(2) of the UK GDPR also provides the data subject with a right to an effective judicial remedy if **the ICO does not handle the complaint or provide the data subject with a progress update within three months**.

Provisions for this are set out in **Section 166** of the DPA 2018. Data subjects may apply to the First Tier Tribunal to make an order against the Commissioner. The order can require the Commissioner to take appropriate steps to respond to the complaint, or inform the complainant of progress or the outcome of the complaint, within a specified period.

Complaints about ICO service

If a data subject is unhappy with the service they receive from the ICO, they can make a complaint. The ICO's website sets out its procedure and deadlines for responding.

If a data subject remains dissatisfied with the ICO's service, or feels that they have not acted properly or fairly, they can refer their complaint to the Parliamentary and Health Service Ombudsman through their local Member of Parliament (MP).