Data Protection and PECR Training

Supporting notes and further reading

Module 13 : The role and powers of the Commissioner

Introduction

These notes are designed to set out the key points covered during module 13 of our data protection online training programme. These notes are not designed to replace the online module, but are intended to be a point of reference for your follow-up study. You may find it helpful to have these notes and the relevant legislation open whilst watching the online module:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)

This document contains:

Supporting notes

Module 13 discusses the role and power of the Commissioner. It covers:

Introduction

The key areas of legislation are:

DPA Part 5	- the Information Commissioner
DPA Part 6	- our enforcement powers
DPA Schedule 12	- the office of the Commissioner
DPA Schedule 13	- general functions
UK GDPR Articles 57 and 58	- the tasks and powers of the Commissioner

The tasks of the Commissioner

Article 57 of the UK GDPR lists the Commissioner's tasks. They include:

- monitor and enforce the application of the UK GDPR;
- promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing – with specific attention given to children;
- upon request, provide information to any data subject concerning the exercise of their rights under the UK GDPR;
- handle complaints lodged by a data subject;

- conduct investigations on the application of the UK GDPR; and
- keep internal records of infringements of the UK GDPR and any corrective measures taken.

Codes of Practice

A key task of the Commissioner is to produce codes of practice in order to promote the awareness of controllers and processors of their data protection obligations.

Sections 121-128 in Part 5 of the DPA gives details of which codes must be produced by the Commissioner. The codes are:

- required by law under the DPA,
- laid before Parliament under specific rules set out within the DPA, and
- published by the Commissioner.

They include:

- the data-sharing code;
- direct marketing code;
- age-appropriate design code ;
- data protection and journalism code.

The Secretary of State may require further statutory codes of practice to be prepared by regulation.

The Commissioner can also decide to produce codes of practice for guidance. For example, the 'code of practice for the use of personal information in political campaigns' falls into this category.

These codes are all found in our guidance pages as they are published.

Handling complaints

Another key task is handling complaints from data subjects if they consider there has been an infringement of the UK GDPR in connection with the processing of their personal data.

The UK GDPR in Part 6 section 165 states that the Commissioner shall:

- handle complaints lodged by a data subject;
- investigate, to the extent appropriate, the subject matter of the complaint;
- inform the complainant of the progress and the outcome of the investigation within a reasonable period; and
- provide an electronic complaint submission form, without excluding other means of communication.

Remember a data subject can also complain to the ICO concerning infringements of Part 3 law enforcement and Part 4 intelligence services processing.

Fees

The fees a controller must pay to the Commissioner are set by the Secretary of State in the 'The Data Protection (Charges and Information) Regulations 2018'.

Every organisation or sole trader who processes personal information must pay a data protection fee to the ICO, unless they are exempt.

There are three tiers of fees payment:

1. Micro organisations in Tier 1 must pay £40 per year. These are organisations with a maximum turnover of £632,000 or no more than 10 members of staff.
2. Small and medium organisations in Tier 2 must pay £60. These have a maximum turnover of £36 million or no more than 250 members of staff.
3. Large organisations in Tier 3 pay £2,900 – these are organisations which do not meet the criteria for tier 1 or tier 2.

Some organisations such as charities and small occupational pension schemes only pay £40 regardless of their size and turnover.

We actively chase non-payers and issue a fixed fine or monetary penalty. These companies and their fines are listed on our website.

We also provide a quick assessment tool so organisations can see if they need to pay a fee.

The Commissioner's investigative powers

Article 58 of the UK GDPR lists the Commissioner's investigative powers, and these include the ability to:

- order the controller and the processor, and where applicable their representative, to provide information for the performance of the ICO's tasks – this is done via an information notice;

- carry out investigations in the form of data protection audits, known as consensual audits; and

- notify the controller or processor of an alleged infringement in an assessment notice.

The ICO is able to obtain access to any premises of a controller and processor, including to any data processing equipment, but needs a judge's warrant to do this.

The Commissioner's corrective powers

The ICO also has corrective powers which include the power to:

- issue warnings to a controller or processor that their intended processing operations are likely to infringe the UK GDPR;

- issue reprimands to a controller or a processor where processing operations have infringed the UK GDPR; and

- use enforcement notices to order a controller or processor to take specific action to bring processing operations into compliance with the UK GDPR within a specified period, or order them to comply with a data subject's requests to exercise his or her data protection rights.

And finally, to:

- impose an administrative fine in a penalty notice, in addition to or instead of the outlined measures.

Please see Article 58 for a complete list of powers.

The Commissioner's approach to enforcement

Our approach to enforcement is laid out in our Data Protection Regulatory Action Policy. This:

- explains when regulatory action will be considered;
- sets out forms of regulatory action available to the ICO;
- gives guidance on when they will be used; and
- is based on risk assessment principles.

Formal action isn't undertaken lightly, and aims to be targeted, proportionate, effective and risk-driven. Our approach is a 'carrot and stick' approach and our aim is to improve compliance.

Our Strategic Threat Assessment or STA is based on the Information Rights Strategic Plan and the Regulatory Action Policy. Its objective is twofold:

- to ensure that the ICO has the right regulatory priorities – this is intended to guide decision-makers in the ICO to help prioritise and direct resources and regulatory effort to those issues that give us most cause for concern; and
- to enable staff to identify and share actionable intelligence across the organisation and externally.

So let's look at how we exercise our civil powers.

Article 58 of the UK GDPR says the Commissioner shall have the power to order the controller and the processor, and where applicable their representative, to provide any information the ICO requires for the performance of its tasks.

So if we require a controller to provide us with information and it is not complying, we can issue an **information notice**.

Sections 142 to 145 of the DPA explain how information notices can and can't be used, what must be included in a notice, and the right of appeal against the notice to the First Tier (Information Rights) Tribunal.

Article 31 of the UK GDPR gives controllers and processors the general obligation to respond to the ICO.

Consensual audits are audits that have been voluntarily agreed between the controller and the Information Commissioner.

They are an assessment of whether the controller or processor is complying with good practice in the processing of personal data. Please see section 129 of the DPA.

They are carried out because:

- the controller has requested one;
- there have been a large number of complaints about the organisation;
- it has been recommended by an investigation; or
- the organisation falls into an ICO campaign area.

These are not to be confused with compulsory audits where the Commissioner issues an assessment notice.

Compulsory assessments or audits

Article 58 gives the Commissioner the power "to carry out investigations in the form of data protection audits."

These are **compulsory** assessments carried out under an assessment notice – to consider whether the controller or processor has complied or is complying with the data protection legislation. They are generally used for investigation purposes and sometimes when consensual audits are refused.

Assessment notices cover any controller or processor, and can be appealed to the First Tier (Information Rights) Tribunal.

They can require the controller or processor to permit the Commissioner to enter specified premises and direct the Commissioner to documents on the premises.

Sections 146 and 147 of the DPA explain how the notices are used to carry out compulsory audits.

An assessment notice must include time scales for when each requirement must be complied with and information about the rights of appeal.

Corrective measures

Article 58 allows the Commissioner to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions of the UK GDPR.

These can't be appealed.

Article 58 also gives the Commissioner the power to issue reprimands to a controller or processor, where processing operations have infringed the provisions of the UK GDPR.

These also can't be appealed.

Example: an organisation might send the ICO a DPIA to review

- the ICO considers that the proposed processing is likely to infringe two UK GDPR principles: principle (a) lawfulness, fairness and transparency and principle (e) storage limitation
- the ICO issues a warning about this processing
- and advises the organisation that failure to comply could lead to formal action being considered, should we receive complaints

Example: an organisation doesn't have appropriate technical and organisational measures in place to ensure the security of its personal data

- this leads to the disclosure of personal data to a member of the public, by mistake
- staff are not adequately trained in data protection
- the personal data breach is not reported within 72 hours
- because of the specifics of the case, the ICO issues a reprimand

Enforcement notices

The Commissioner can use an enforcement notice to order controllers and processors to:

- comply with the data subject's requests to exercise his or her data protection rights;
- bring processing operations into compliance with the UK GDPR, within a specified period;
- communicate a personal data breach to the data subject;
- impose a temporary or definitive limitation including a ban on processing; and
- order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data has been disclosed.

Sections 149-153 of the DPA gives the detail of how enforcement notices can and can't be used, what must be included in a notice, and the right of appeal against the notice to the First Tier (Information Rights) Tribunal.

For example, an enforcement notice we issued ordered an organisation to stop processing biometric data in the form of automatic voice recognition. These notices are published on our website.

Administrative fines

Article 83 outlines the conditions for imposing administrative fines. There are two tiers of fines:

The Higher Tier concerns infringements around the obligations, for example on:

- the basic principles for processing, including conditions for consent;
- data subjects' rights;
- international transfers; and
- non-compliance with the Commissioner's investigative and corrective powers.

The Lower Tier infringements are mainly concerned with the failure to meet organisational obligations, for example to:

- appoint data protection officers;
- maintain written records;
- implement appropriate technical and organisational measures to ensure security of processing; and
- report breaches where required to do so.

Note the higher tier infringements focus on the individual whereas the lower tier focus on the organisational obligations.

The higher tier allows administrative fines up to £17,500,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The lower tier allows administrative fines of up to nearly £9,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover.

Article 83 says that where administrative fines are imposed they must be: effective, proportionate, and dissuasive.

When imposing a fine, the factors which should be considered include:

- the number of people involved;
- any damage to the data subjects;
- the negligent or intentional character of the infringement;
- action taken by the controller to mitigate the damage;
- the controller's level of adherence to codes of conduct and approved certification mechanisms; and
- the extent to which the controller notified the ICO of the infringement and co-operated with it.

We publish the fines we impose on our website.

Civil investigations

Our civil investigations generally stem from a self-reported personal data breach or a complaint made to the ICO.

To conduct an investigation, case officers review all the available information and then send enquiries to the controller to fill any gaps in knowledge about an incident.

The enquiries usually focus on what has happened, why it happened and the controller's policies, procedures and training.

A civil investigation report will include information such as

- a description of the incident;
- basic case information including breach reporting;
- third party involvement (domestic and overseas);
- complaints and data subject notification; and
- initial lines of enquiry.

This kind of information will be used to decide if regulatory action is necessary.

Criminal offences in the DPA

There are a number of criminal offences in the DPA. They include:

- Confidentiality of information - this applies to us as staff at the ICO. It means, for example, that we must not disclose information which has been obtained by, or provided to, the ICO in the course of discharging the Commissioner's functions.

  This includes disclosure by us to other regulators - we need a lawful basis to do this.

- False statements made in response to information notices are also criminal offences.

- Destroying or falsifying information and documents (such as information and assessment notices).

- Unlawfully obtaining personal data. This includes obtaining, disclosing, procuring, selling and offering to sell personal data without the consent of the controller.

- Re-identification of de-identified personal data.

- The alteration of personal data to prevent disclosure to a data subject.

Remember the controller is the victim of the criminal offence in these cases, not the data subject.

Example: criminal offences under the DPA

- a hospital employee copies the medical records of a famous person
- an employee steals a database of personal data when they leave for a job with a rival company
- an employee sells a list of contact numbers to another organisation without the controller's knowledge or consent
- an organisation destroys information requested by the ICO in an Information Notice
- a DPO alters records to avoid disclosing personal data in response to a SAR
- an employee re-identifies personal data which has been de-identified and then discloses the data to someone else

Powers of entry and inspection

Schedule 15 of the DPA addresses the Commissioner's powers of entry and inspection and the issue of warrants in connection with non-compliance and offences. For example, warrants are granted by judges to the Commissioner and can authorise the Commissioner or ICO staff to:

- enter and search premises;
- inspect, examine, test, operate any equipment used to process personal data; and
- seize documents or other material as evidence.

Other pieces of legislation

Other pieces of legisaltaion that our criminal investigations staff have to comply with when investigating offences under DP law include the:

- Criminal Procedures and Investigations Act;
- Police and Criminal Evidence Act;
- Human Rights Act;
- Investigatory Powers Act;
- Victims Code.

The burden of proof in criminal cases is higher than in civil ones. It has to be 'beyond reasonable doubt' that the offence has been committed. In civil cases it has to be on the 'balance of probabilities'.

The staff dealing with the prosecutions of cases will also have to be aware of the criminal court processes in England, Wales and Northern Ireland. There is a different process in Scotland.

Example: an organisation reports a cyber incident to the ICO

- it explains that user traffic to its website had been diverted to a fraudulent site
- the attackers harvested customer details, compromising the personal data of 500,000 customers
- the controller had poor security arrangements to protect payment details and name and address data
- the ICO issued a substantial fine on the controller

Example: an organisation reports a large backlog of unanswered SARs

- it has more than 1,100 open requests, with nearly 680 over three months old
- the ICO issued two enforcement notices ordering the controller to clear the backlog by a certain time
- the controller was asked to change its internal systems, procedures and policies and to improve its SAR handling systems, including the reporting of delays to data subjects
- it put a recovery plan in place and committed to addressing the backlog

Example: an organisation fails to keep the personal data held on its network secure

- an employee lost a memory stick which was found by a member of the public
- this contained over 1,000 files which were not encrypted or password protected, and included the names, dates of birth and passport details of 10 individuals, plus details of 50 security personnel
- these were passed on the stick to a national newspaper and were copied before its return
- the ICO issued a substantial penalty fine

For the levels of different fines imposed, please see the ICO website under the section '[Action we've taken]'.

Back to top

Further reading

In the key data protection themes section of our website, have a look at the sections on the Age Appropriate Design Code and the Data Sharing Information Hub.

You should then look at the action we've taken section on our website, and read about:

- the different types of enforcement action we've taken – using the tab at the side of the page to filter by monetary penalties, enforcement notices and prosecutions; and
- the audits and overview reports that we've produced.

You should then look at different investigations that are ongoing, and investigations such as the use of data analytics for political purposes and compliance in the direct marketing data broking sector.

You should then read through our Regulatory Action Policy.

Lastly, have a look at the page setting out our strategies and plans, including our Openness by design, and Information rights strategic plans.

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022