Data Protection Regulatory Action Policy

Why a policy?

The information rights strategy for the Information Commissioner's Office (ICO) commits us to adopting a positive and proactive approach to ensuring compliance by:

- helping and encouraging organisations to understand and meet their information rights obligations more easily;
- responding proportionately to breaches of information rights law.

This 'carrot and stick' approach means that we will adopt a targeted, risk-driven approach to regulatory action - not using our legal powers lightly or routinely, but taking a tough and purposeful approach on those occasions where that is necessary.

This Regulatory Action Policy sits under the umbrella of our information rights strategy. It elaborates the above approach, setting out the nature of our various powers and when and how we plan to use them. The ICO intends that this policy should send clear and consistent signals to those who fall within the scope of the Data Protection Act 1998 (the Act), Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended (PECR) and related laws, to the public whom the law protects and empowers, and to the staff who act on the ICO's behalf.

What is regulatory action?

The ICO has powers to change the behaviour of organisations and individuals that collect, use and keep personal information. These powers are designed to promote compliance with the Act, PECR and related laws. They include criminal prosecution, civil monetary penalties, non-criminal enforcement and, in some circumstances, audit. Regulatory action is the term used to describe the exercise of these powers.

Our aim

Our aim is to ensure that personal information is properly protected. We will do so by taking purposeful regulatory action where this is at risk because:

• obligations are deliberately or persistently ignored; or
• examples need to be set; or
• interpretation of the law is in doubt.

Targeted, proportionate and effective regulatory action will also contribute to the promotion of good practice and ensuring we remain an influential office.

Guiding principles

In line with our information rights strategy, the ICO follows the five principles of good regulation. These are that regulatory activities should be carried out in a way which is transparent, accountable, proportionate and consistent; and that regulatory activities should be targeted only at cases in which action is needed. Further detail of how we apply these principles is set out in Appendix A.

The ICO will also have regard to the provisions of the Regulators' Compliance Code, (and the Regulators' Code which will succeed it). The code applies when regulators determine their general policies or principles about exercising their regulatory functions and when setting standards or giving general guidance in a regulatory context. This policy is designed to give effect to the relevant provisions of the code.

In the case of criminal conduct we will follow the Code for Crown Prosecutors and publish the ICO's own prosecution policy statement.

More generally our aim will be to publicise the regulatory action we take so as to educate data controllers and others and drive good data protection practice.

Forms of regulatory action

There are a number of tools available to the ICO for regulatory action. Where a choice exists, the most effective will be chosen for each situation, bearing in mind the deterrent or educative effect on other organisations. The tools are not necessarily mutually exclusive. They will be used in combination where justified by the circumstances. The main options include an enforcement notice, monetary penalty notice, audit and criminal prosecution. Further details of the tools available are set out in Appendix B.

Initiation of regulatory action

We will adopt a selective approach to initiating and pursuing regulatory action whether the action is initiated by ourselves or in response to matters raised with us by others. Our approach will be driven by concerns

about significant actual or potential detriment caused by non-compliance with data protection principles, the PECR or other relevant legal requirements. The criteria set out below will guide decisions about our priorities at all stages – fact-finding, initiation of action and follow-through. We will always be clear about the outcome(s) we are aiming to achieve.

The initial drivers will usually be:

- issues of general public concern (including those raised in the media);
- concerns that arise because of the novel or intrusive nature of particular activities;
- concerns raised with us in complaints that we receive;
- concerns that become apparent through our other activities.

In setting priorities for regulatory action we will pay particular attention to the priority sectors or activities identified for particular regulatory attention in our information rights strategy. The current information rights priority areas are listed here. We will supplement this by collecting intelligence and undertaking compliance checks with a view to identifying more specific sectors or organisations for targeted activity. In selecting areas for attention we will bear in mind the extent to which market forces can themselves act as a regulator. Thus the public sector, particularly where processing is hidden from view, where individuals have little or no choice and where sensitive personal data are involved might well receive more attention from us than the private sector.

We will work closely with other UK regulators where we have a shared interest in regulatory action, developing and publishing details of memoranda of understanding and other collaborative arrangements. We will also work with data protection authorities in other countries to co-ordinate the initiation and pursuit of regulatory action in appropriate cases. One of our incentives will be the benefits of achieving a consistent and joined up approach to cross-border enforcement particularly within the European Union.

Complaints received about breaches of the law by organisations or individuals will be one of our drivers for regulatory action but not all complaints where it appears that compliance is unlikely will be referred for regulatory action. We will build up intelligence based on the number and nature of complaints received about particular organisations. Cases will only be taken on in the ICO's Good Practice and Enforcement Departments where:

- our criteria are satisfied; and

- either a monetary penalty, a sanction for a criminal breach or other formal action to bring about compliance is both a proportionate response and an outcome that is reasonably achievable; or
- an audit could be expected to bring about any necessary improvement in practice.

Consensual vs. compulsory audits

Audits are undertaken in a variety of circumstances, not all of which will amount to regulatory action. The ICO does see auditing as a constructive process with real benefits for data controllers and so aims to establish, wherever possible, a participative approach. We will usually seek the agreement of a data controller to a consensual audit in the first instance. Only where data controllers are unusually unwilling to engage and risks have been identified will we use our power to issue an assessment notice and conduct a compulsory audit.

Furthermore, we will not place unreasonable demands on organisations that are selected for audit attention. In return for this approach we expect organisations to co-operate with us even if they are not under a legal obligation to do so. We will be prepared to identify organisations where we do not receive a reasonable level of co-operation. If a data controller fails to agree to an audit without a good reason this may be taken into account when determining the amount of any monetary penalty, if an audit could reasonably have been expected to reveal the risk of the contravention at issue.

In return data protection audit services will be conducted by trained and competent auditors employed by or contracted to the ICO. Further, the ICO will not impose a monetary penalty in respect of any contravention discovered in the process of carrying out either a consensual or compulsory audit.

Code of Practice on assessment notices

The ICO will use the power to carry out compulsory audits where risks are identified and data controllers are unwilling to engage consensually. This power only extends to government departments, any designated public authorities and organisations within any other designated categories.

The ICO is required to prepare and issue an assessment notice code of practice which has been approved by the Secretary of State. The code of practice sets out the factors that will inform the ICO's decision to serve an assessment notice on a data controller and specifies how compulsory audits will be conducted. Information relating to the ICO's risk based approach to audit is included in this code of practice.

The ICO will take broadly the same approach to consensual audits as to compulsory audits. Where there are differences these are highlighted in the code.

Guidance on monetary penalties

The ICO will use its power to serve monetary penalty notices to deal with serious contraventions of the data protection principles and of PECR. It will be used as both a sanction and a deterrent against data controllers or persons who deliberately or negligently disregard the law.

The ICO is required to issue guidance on how it proposes to exercise its power to serve monetary penalty notices which has been approved by the Secretary of State and both Houses of Parliament and which is available on the ICO website. The guidance deals with the circumstances in which the ICO would consider it appropriate to serve a monetary penalty notice, and how it will determine the amount of the monetary penalty. It is based on the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

If a monetary penalty notice has been served on an organisation the ICO may still serve an enforcement notice in relation to the same contravention if it is satisfied that positive steps need to be taken by the data controller in question to achieve compliance with the data protection principle(s) and/or PECR.

Decision making

We will ensure that regulatory action we take is proportionate to the mischief it seeks to address. Both good regulatory practice and the efficient use of our limited resources require us to be selective. In determining whether to take action, the form of any action and how far to pursue it, we will apply the following criteria:

- Is the past, current or prospective detriment for a single individual resulting from a 'breach' so serious that action needs to be taken?

- Are so many individuals adversely affected, even if to a lesser extent, that action is justified?

- Is action justified by the need to clarify an important point of law or principle?

- Is action justified by the likelihood that the adverse impact of a breach will have an on-going effect or that a breach will recur if action is not taken?
- Is the organisation and its practices representative of a particular sector or activity to the extent that the case for action is supported by the need to set an example?

- Does the novel, precedent setting or particularly intrusive nature of the practices in question mean that an example needs to be set?

- Is the likely cost to the organisation of taking the remedial action required reasonable in relation to the issue at stake?

- Does a failure by the organisation to follow relevant guidance, a code of practice or accepted business practice support the case for action?

- Does the attitude and conduct of the organisation both in relation to the case in question and more generally in relation to compliance issues suggest a deliberate, wilful or cavalier approach?

- How far do we have a responsibility to organisations that comply with the law to take action against those that do not?

- Would it be more appropriate or effective for action to be taken by other means (e.g. another regulator, legal action through the courts)?

- Is the level of public interest in the case so great as to support the case for action?

- Given the extent to which pursuing the case will make demands on our

resources, can this be justified in the light of other calls for regulatory action?
- What is the risk to the credibility of the law or to our reputation and influence of taking or not taking action?

We will give organisations an opportunity to make representations to us before we take regulatory action that affects them unless matters of urgency or other circumstances make it inappropriate to do so.

The Enforcement section of our website contains many examples of the circumstances in which we have taken regulatory action. Attached to this policy in Appendix C are some illustrative examples of where we are not likely to take regulatory action.

Cases involving processing for the special purposes

The policy applies to all sectors and all organisations and individuals that are processing personal information within the scope of the Act. This includes the press, other media organisations and anyone else processing personal data for the special purposes (ie the purposes of journalism, artistic purposes and literary purposes). However, in recognition of the importance of the public interest in freedom of expression, the ICO's powers to take regulatory action are restricted where personal data are processed only for the special purposes.

In essence, the ICO cannot serve an enforcement notice to prevent the publication of journalistic, literary or artistic material that has not previously been published. Before the ICO can serve an enforcement notice we must not only make a determination that the personal data in question are not being processed only for the special purposes or are not being processed with a view to publication but also obtain leave from a court for the notice to be served. Before granting leave the court has to be satisfied that the contravention of the data protection principles being addressed is of substantial public importance. Subject to these significant restrictions, and the need to have proper regard for the public interest in freedom of expression, the ICO is committed to taking regulatory action in accordance with this policy against the press and other media organisations, just as it would against data controllers in other sectors where this is necessary to ensure compliance with the requirements of the Act.

So far as criminal cases involving media organisations or individual journalists are concerned the ICO will, in addition to the Code for Crown Prosecutors and our own prosecution policy statement, have regard to the

CPS Guidelines for prosecutors on assessing the public interest in cases affecting the media.

Delivery

The Director of Operations will have primary responsibility for delivery in accordance with this policy. The Director will do so mainly through three departments:

Good Practice Department	Responsible for systematically checking an organisation's compliance with the requirements of good practice, in particular through audit activity.
Enforcement Department	Responsible for investigating and taking action in both civil enforcement and criminal cases, including the issuing of enforcement notices or monetary penalty notices where appropriate, and the investigation and prosecution of criminal breaches of the Act.
Complaints Resolution Department	Responsible for investigating and taking action in some civil enforcement cases, including the issuing of enforcement notices and undertakings where appropriate.

The Good Practice, Enforcement and Complaints Resolution Departments will work closely together and with other parts of the ICO, including the Policy Delivery and Strategic Liaison Departments, which may be giving on-going guidance to the same organisations that may be considered for regulatory action. Technical expertise to support regulatory action will be provided by the Information Rights Technology Team.

In the interests of effective and efficient working the Information Commissioner will give delegated authority to one or both of the Deputy Commissioners acting in consultation with the Head of Enforcement to serve enforcement notices and monetary penalty notices. The Information Commissioner will also give delegated authority to the Deputy Commissioner (Director of Data Protection) acting in consultation with the Head of Good practice to serve assessment notices. The Information Commissioner will give delegated authority to the Head of Enforcement to issue Section 159 notices and information notices.

Transparency

In line with the ICO's commitment to transparency we will be open about regulatory action we take. We will make information available on the ICO's website and in the annual report to Parliament about the number of cases we pursue, their nature and the outcomes. We will normally publish monetary penalty notices, enforcement notices, undertakings, assessment notices and the outcome of prosecutions with any confidential or commercially sensitive information redacted. The extent to which we will publish information about our audit activities is covered by the code of practice on assessment notices.

Where regulatory action reveals problems that are common to a particular business sector or activity and it is apparent that there is a need for general advice on the issue in question we will make such advice available.

Measurement and Evaluation

The ICO's information rights strategy commits us to doing all we can to measure our effectiveness in delivering the ICO's desired information rights outcomes and adapting if we find we are falling short. In the context of regulatory action we will take steps to measure how effective the use of our powers is in bringing about compliance with the law and the following of good data protection practice. Specific methods we will use to measure our effectiveness are set out in our information rights strategy.

Appendix A

GUIDING PRINCIPLES

Regulatory action taken by the ICO will be consistent with the five Principles of Good Regulation. These are:

Transparency	We will be open about our approach to regulatory action and open about the action we take and the outcomes we achieve.
Accountability	We will include information on the use of our regulatory action powers in our annual report to Parliament. We will make sure that those who are subject to regulatory action are aware of their rights of appeal.
Proportionality	We will put in place systems to ensure that regulatory action we take is in proportion to the harm or potential harm done. We will not resort to formal action where we are satisfied that the risk can be addressed by negotiation or other less formal means.
Consistency	We will apply our decision making criteria consistently in the exercise of our regulatory action powers.
Targeting	We will target regulatory action on those areas where it is the most appropriate tool to achieve our goals. Our own targets will be based on outcomes rather than how often we use our regulatory action powers.

Appendix B

FORMS OF REGULATORY ACTION

Criminal prosecution	A sanction available where there has been a criminal breach of the Act (Section 60 of the Act).
Caution	An alternative to prosecution where a criminal offence under the Act has been admitted but a caution is a more appropriate response than prosecution.
Monetary Penalty Notice	A formal notice requiring an organisation to pay a monetary penalty of an amount determined by the Information Commissioner which must not exceed £500,000 (Section 55A – E of the Act and Regulation 31 of the PECR).
Fixed Monetary Penalty Notice -PECR	A formal notice requiring communications service provider to pay a fixed monetary penalty of £1,000 for failing to comply with the personal data breach notification requirements of PECR (Regulation 5C of the PECR).
Enforcement Notice	A formal notice requiring an organisation or individual to take the action specified in the notice in order to bring about compliance with the Act and related laws. Failure to comply with a notice is a criminal offence (Section 40 of the Act and Regulation 31 of the PECR).
Section 159 Order	An order requiring a credit reference agency to add a 'notice of correction' to a consumer's file (Section 159 Consumer Credit Act 1974).
Application for an injunction	An injunction issued by a court under the Unfair Terms in Consumer Contracts Regulations 1999 to prevent the continued use of an unfair contract

	term (Regulation 12 Unfair Terms in Consumer Contract Regulations 1999).
Application for an Enforcement Order	An order issued by a court requiring a person to cease conduct harmful to consumers. (Section 213 Enterprise Act 2002).
Audit – consensual	An assessment, made with the agreement of an organisation, as to whether the organisation's processing of personal data follows good practice (Section 51(7) of the Act).
Audit – compulsory	An assessment, made following the issuing of an assessment notice, as to whether an organisation has complied or is complying with the data protection principles (Section 41A of the Act).
Audit - PECR	A compulsory audit of the compliance of a communications service provider with the personal data breach requirements of PECR (Regulation 5B of the PECR)
Negotiated Resolution	Not a statutory regulatory power but negotiated resolution will be used widely in order to bring about compliance with the Act, PECR and related laws. Negotiated resolution can be supported by an undertaking.
Undertaking	Not a statutory regulatory power but a formal undertaking can be given by an organisation to the ICO committing the organisation to a particular course of action or otherwise achieving compliance.

The ICO also has powers that can be used in connection with regulatory action. These are:

Information Notice	A notice requiring an organisation or person to supply the ICO with the information specified in the notice for the purpose of assessing whether the Act or related laws have been complied with. Failure to comply with a notice is a criminal offence (Sections 43 and 44 of the Act and Regulation 31 of the PECR).
Special Information Notice	A form of information notice requiring an organisation or person to supply the ICO with information needed to ascertain whether personal data are being processed for the special purposes ie the purposes of journalism, artistic purposes or literary purposes (Section of 44 of the Act).
Third Party Information Notice	A form of information notice requiring a communications provider to supply the ICO with information specified in the notice about another person's use of electronic communications where this is necessary to investigate compliance of any person with the PECR (Regulation 31A of the PECR).
Assessment Notice	A notice served on government departments, any designated public authorities or any other organisations within designated categories for the purpose of enabling the Information Commissioner to determine whether the data controller has complied or is complying with the data protection principles i.e. to enable the carrying out of a compulsory audit (Section 41A of the Act).
Search warrant	Powers of entry, inspection and seizure on application to a judge, where there are reasonable grounds for suspecting an

	offence under the Act has been committed or the data protection principles or PECR have been contravened (Section 50 and Schedule 9 of the Act and Regulation 31 PECR).
Authorisation to access communications data or to undertake directed surveillance.	An authorisation issued under the Regulation of Investigatory Powers Act 2000 (RIPA) to enable the ICO to gain lawful access to communications data where it is necessary and proportionate to do so for the purposes of the detection or prevention of crime (Sections 22 & 28 of RIPA).

Appendix C

REGULATORY ACTION EXAMPLES

The following are some examples of the types of conduct which are unlikely to lead the ICO to use its formal regulatory powers. The examples are intended to be illustrative rather than exhaustive or binding. In practice all the relevant circumstances of a case will be taken into account. The ICO's website contains many examples of the circumstances in which we have taken regulatory action.

- Non-compliance with the data protection principles, but where the Data Controller has taken reasonable steps in the circumstances to prevent a breach.

- Single non-criminal breaches by small businesses caused by ignorance of requirements.

- Non-criminal, non-compliance which is not particularly intrusive and has not caused significant detriment.

- Breaches arising from commercial disputes which are minor in nature, for example those which can be resolved by other means such as a private civil action.