Data Protection Regulatory Action Policy

Why a policy?
The over-riding data protection imperative of the Information Commissioner's Office (ICO) is to *"take a practical down to earth approach – simplifying and making it easier for the majority of organisations who seek to handle personal information well and tougher for the minority who do not."* This 'carrots and sticks' 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 elaborates that 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 data protection 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 bring about compliance with the Data Protection Act 1998 (the Act) and related laws. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller. 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
- issues need to be clarified.

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

Guiding principles
Regulatory action taken by the ICO will be consistent with the five Principles of Good Regulation established by the Better Regulation Task Force. 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.

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 are:

Criminal prosecution	A sanction available where there has been a criminal breach of the Act (Section 60 Data Protection Act 1998).
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.
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 Data Protection Act 1998 and Regulation 31 Privacy and Electronic Communications (EC Directive) Regulations 2003).
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 Data Protection Act 1998).
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) Data Protection Act 1998).
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 Data Protection Act 1998).
Negotiation	Not a formal regulatory power but a form of regulatory action that will be used widely in order to bring about compliance with the Act and related laws. Negotiated resolution can be backed by a formal undertaking given by an organisation to the ICO.

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 Data Protection Act 1998 and Regulation 31 Privacy and Electronic Communications (EC Directive) Regulations 2003).
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 Data Protection Act 1998).
Search warrant	Powers of entry and inspection, 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 have been contravened (Section 50 and Schedule 9 Data Protection Act 1998).

Initiation of regulatory action

We will adopt a selective approach to initiating and pursuing regulatory action. Our approach will be driven by concerns about significant actual or potential **detriment** caused by non-compliance with data protection principles 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.

We will initiate regulatory action ourselves, as well as in response to matters raised with us by others. We will undertake compliance checks with a view to identifying sectors or specific organisations for more focused 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 and where the risks of a 'surveillance society' may be greater, might well receive more attention from us than the private sector.

Through these compliance checks and information that we gain from our other activities we will target particular sectors or organisations for attention. This will include audit. We will work with data protection authorities in other countries to co-ordinate the initiation of regulatory action in appropriate cases.

Complaints received about breaches of the law by organisations or individuals will be one driver for regulatory action. 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 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

The ICO sees 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 of either a consensual or compulsory audit. We will also examine whether meaningful benefits such as some form of accreditation can be offered to organisations that make use of such services or co-operate with us in other ways.

Code of Practice on assessment notices
The ICO intends to 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 and will be available on the ICO website. 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 intends to use its power to serve monetary penalty notices to deal with serious contraventions of the data protection principles. It will be used as both a sanction and a deterrent against data controllers 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 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 also 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).

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 ongoing 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?
- 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.

Attached to this policy are some illustrative examples of where we will or will not be likely to take regulatory action.

Delivery
The Director of Operations will have primary responsibility for delivery in accordance with this policy. The director will do so mainly through two 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 non-criminal enforcement action in cases where it is not possible or it is inappropriate to achieve remedial action by negotiation; the issue of monetary penalty notices where appropriate; the investigation, initial assessment and co-ordination, of pre-prosecution work in criminal cases.

These functions will require a mix of skills which will be brought to bear on project work that runs across more than one department. This will include compliance checks and investigations.

In the interests of effective and efficient working the Information Commissioner will give delegated authority to the Deputy Commissioner (Director of Data Protection) 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.

The Good Practice and Enforcement Departments will work closely with other parts of the office. In particular this will involve the Complaints Resolution Department from which the Good Practice Division and Enforcement Division will receive much of their work and the Strategic Liaison Department which may be giving guidance to the same organisations that may be considered for regulatory action.

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.

Regulatory action examples
The following are some examples of the types of conduct which will lead the ICO to consider using 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 and, in the case of criminal conduct, the Code for Crown Prosecutors will be followed.

Likely (especially after warning)

- Repeated failure to take adequate security measures.
- Collecting and retaining detailed or sensitive personal information on a 'just in case' basis.
- Inaccurate or long out-dated information which impacts on career prospects.
- Seriously intrusive marketing – e.g. repeated failure to observe Telephone Preference Service requirements.
- 'Professional' breaches of Section 55 (unlawful obtaining) e.g. by private investigation agencies.
- Failure to notify despite reminders.
- Denial of subject access where it is reasonable to suppose significant information is held.

Unlikely

- 'Accidental' non-compliance with the data protection principles – which is recognised and where effective remedial action is swiftly taken.
- Single non-criminal breaches by small businesses caused by ignorance of requirements.
- Non-compliance which is not particularly intrusive and has not caused significant detriment – e.g. a single mail shot.
- Non-compliance where other pressures – e.g. damage to reputation, may be swifter and more effective than action by a regulator.
- Business vs. business disputes where there is no detriment to customers.
- 'Domestic' breaches of Section 55 (unlawful obtaining) e.g. feuding spouses or work colleagues – except where a significant abuse of trust is involved.