Information Commissioner's Office

Promoting public access to official information
and protecting your personal information

A STRATEGY FOR DATA PROTECTION REGULATORY ACTION

WHY A STRATEGY?

The over-riding data protection imperative of the Information Commissioner's Office 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 Strategy elaborates that approach, setting out the nature of our various powers and when and how we plan to use them. The Commissioner intends that this Strategy 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 his behalf.

WHAT IS REGULATORY ACTION?

The Information Commissioner 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. 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 Information Commissioner 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 Information Commissioner for Regulatory Action. Where a choice exists, the most effective will be chosen for each situation, bearing also in mind the deterrent or educative effect on other organisations. 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).
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	-	An assessment made, with the consent of an organisation, as to whether the organisation's processing of personal data follows good practice (Section 51(7) Data Protection Act 1998).
Inspection	-	An inspection of personal data recorded in certain European law enforcement systems in order to check compliance with the Act (Section 54A 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 Commissioner.

The Commissioner also has powers available to him that can be used in connection with Regulatory Action. These are:

Information Notice	-	A notice requiring an organisation or person to supply the Commissioner 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).
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 focussed 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 other EU data protection authorities, to coordinate the initiation of Regulatory Action in appropriate cases.

We will not place unreasonable demands on organisations that are selected for attention. In return 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. In return we will work with outside providers to encourage and support the development of reputable data protection audit services. We will also examine whether we can offer meaningful benefits to organisations that make use of such services or co-operate with us in other ways.

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 Regulatory Action Division where:

- our criteria are satisfied; and
- either 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.

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?

- are 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 strategy are some illustrative examples of where we will or will not be likely to take Regulatory Action.

DELIVERY

The Regulatory Action Division will be charged with delivery of this strategy. It will do so through four units:

- Remedies Unit	-	Responsible for the negotiated resolution of non-criminal cases where there appears to be a breach of the law and remedial action is required from the organisation in question.
- Audit Unit	-	Responsible for systematically checking an organisation's compliance with the requirements of good practice.
- Enforcement Unit	-	Responsible for non-criminal enforcement action in cases where it is not possible or it is inappropriate to achieve remedial action by negotiation. Responsible for the initial assessment and co-ordination, of pre-prosecution work in criminal cases.
- Investigations Unit	-	Responsible for bringing professional investigatory skills to bear on all aspects of the Division's work, in particular in relation to 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 unit. This will include compliance checks.

In the interests of effective and efficient working the Commissioner will give delegated authority to the Deputy Commissioner (Data Protection) acting in consultation with either the Legal Director or Principal Solicitor to issue enforcement notices. He will give delegated authority to the Head of the Regulatory Action Division and the Head of Remedies and Audit to issue Section 159 notices.

The Regulatory Action Division (RAD) will work closely with other parts of the office. In particular this will involve the Casework and Advice Division from which RAD will receive much of its work and the Guidance and Promotion Division (GPD) which will be giving guidance to the same organisations that RAD will be considering for Regulatory Action.

EU THIRD PILLAR

The "Third Pillar" is the area of EU actually concerned with cooperation in the fields of justice and home affairs. Within the Third Pillar there are several European law enforcement institutions including Europol, Eurojust, the Schengen Information System and the Customs Information System. Each of these institutions has its own data protection supervisory body on which the Information Commissioner is represented. We are committed to making an active and effective contribution to these regulatory activities at European level. This work will be supported by the Regulatory Action Division.

TRANSPARENCY

In line with the Information Commissioner's Transparency Policy we will be open about Regulatory Action we take. We will make information available on the number of cases we pursue, their nature and the outcomes. We will also publish an occasional bulletin summarising the details of illustrative cases that have been considered for Regulatory Action.

In some cases, particularly where audit is involved; we must currently rely on the consent of an organisation as the basis for Regulatory Action. In these circumstances we may be willing to give the organisation concerned an undertaking of confidentiality subject to our reserving the right to act on serious breaches of the law and to comply with legal obligations placed on us.

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 Information Commissioner to consider using his 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.