THE OFFICE OF THE
Data Protection Commissioner

Data Protection Regulatory Action Policy

Why a policy?

The over-riding data protection imperative of the Data Protection Commissioner's Office (DPCO) 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 DPCO 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 DPCO's behalf.

What is regulatory action?

The DPCO 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 (Jersey) Law 2005 (the Law) 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 ICO will be consistent with the five Principles of Good Regulation established by the Better Regulation Task Force. These are:

1. Transparency

We will be open about our approach to regulatory action and open about the action we take and the outcomes we achieve;

2. 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.

3. 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.

4. Consistency

We will apply our decision making criteria consistently in the exercise of our regulatory action powers.

5. 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 DPCO 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 Law (Article 61 Data Protection (Jersey) Law 2005).

- **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 Law and related laws. Failure to comply with a notice is a criminal offence. (Article 40 Data Protection (Jersey) Law 2005).

- **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 Law and related laws. Negotiated resolution can be backed by a formal undertaking given by an organisation to the DPCO.

The DPCO 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 DPCO with the information specified in the notice for the purpose of assessing whether the Law or related laws have been complied with. Failure to comply with a notice is a criminal offence. (Article 43 Data Protection (Jersey) Law 2005).

- **Special Information Notice**

A notice requiring an organisation or person processing personal data for special purposes to supply the DPCO with the information specified in the notice for the purpose of assessing whether the Law or related laws have been complied with. Failure to comply with a notice is a criminal offence. (Article 44 Data Protection (Jersey) Law 2005).

- **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. (Article 50 and Schedule 9 Data Protection (Jersey) Law 2005).

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.

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

In the interests of effective and efficient working the Data Protection Commissioner will give delegated authority to the Deputy Commissioner to serve information and enforcement notices and issue undertakings.

Transparency

In line with the DPCO's commitment to transparency we will be open about regulatory action we take. We will make information available on the DPCO's website and in the annual report to the States of Jersey about the number of cases we pursue, their nature and the outcomes. We will publish enforcement notices, undertakings, and the outcome of prosecutions where it is appropriate to do so with any confidential or commercially sensitive information redacted.

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 DPCO 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, cases will be referred to the Attorney General.

<u>Likely (especially after warning)</u>

- 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 Article 55 (unlawful obtaining) e.g. by private investigation agencies.
- 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.