DATA PROTECTION POWERS AND PENALTIES

The Case for Amending the Data Protection Act 1998

Summary

This paper sets out the Information Commissioner's case for changes to be made to the Data Protection Act 1998 (the Act) to create:

- a penalty for knowingly or recklessly failing to comply with the data protection principles so as to create a substantial risk that damage or distress will be caused to any person

- a power for the Information Commissioner to inspect personal data and the circumstances surrounding its processing in order to assess whether or not any processing of the data is carried out in compliance with the Act.

- a power for the Information Commissioner to require a data controller to provide him with a report by a skilled person

- enhanced enforcement powers to enable the Information Commissioner to bring seriously unlawful processing to an immediate halt, to place formal undertakings on a statutory basis and to enable the Information Commissioner to take enforcement action to prevent breaches of the Act that are likely to occur
- information notices that can be served on any person rather than just a data controller.

The Commissioner submits that introducing these changes would significantly increase the ability of his office to deliver its commitment to:

"Strengthening public confidence in data protection by taking a practical, down-to-earth approach - making it easier for the majority of organisations who seek to handle personal information well and tougher for the minority who do not".

The additional but limited powers and penalties outlined above are very unlikely to be controversial in party political terms. They would help put the Information Commissioner's Office (ICO) on a comparable footing to other UK regulators and to other EU data protection authorities whilst at the same time helping the Government to meet its commitment to build a regulatory regime in the UK that is effective, flexible and proportionate in tackling the mischiefs to which it is directed. They would also be a significant step forward in modernising the UK's data protection regime by reflecting, in the powers of the regulator and the penalties that can be imposed, the enormous growth that has taken place in the collection and use of personal information and the associated potential for harm that can arise from unlawful processing. Most importantly they would send a clear message that data protection

requirements can not be ignored or dismissed. They must be taken seriously by every organisation that processes personal information.

Existing Penalties

The sanctions currently available to the Information Commissioner under the DPA are primarily concerned with bringing an organisation's future conduct into compliance with the Act. For the most part they do not allow a penalty to be imposed for breaches that have already taken place. This is true not only of the power to issue enforcement notices under Section 40 of the Act but also of powers the Commissioner has under other legislation, most notably those under Part 8 of the Enterprise Act 2002, including the power to seek an enforcement order, exercisable by the Commissioner as a designated enforcer in relation to enforcement of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "PECR Regulations"). These enforcement powers are, and will continue to be, an important regulatory tool for the Commissioner. Where an organisation has acted responsibly but has misunderstood or misapplied the Act, where it has taken a considered but different view of the requirements of the Act from that taken by the Commissioner or where the consequences of a breach are less serious an order requiring future compliance is an appropriate and proportionate sanction.

In some limited areas the Act creates criminal offences for which the Commissioner can prosecute. These are generally where the mischief being addressed is sufficiently serious to warrant a criminal penalty both as a means of punishing those responsible for the wrongdoing and as a means of deterring others. The principal offences are:

- Section 17 - processing without a registration

- Section 55 - unlawful obtaining etc. of personal data.

These offences are currently punishable by a fine of up to £5000 in a Magistrates' court or an unlimited fine in the Crown Court. Legislation to introduce the possibility of a custodial sentence for a Section 55 offence is now before Parliament.

The Act binds the Crown but government departments are not liable to prosecution. However a person in the service of the Crown can commit and be prosecuted for a section 55 offence. More generally where an offence can be proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of a body corporate that person can be prosecuted.

There is though a shortfall in the sanctions available to the Information Commissioner and the means of enforcing those sanctions swiftly and effectively. There is no effective punishment or deterrent available for those who knowingly or recklessly disregard the requirements of data protection law in a way that causes a significant risk of harm whether directly to individuals or indirectly by undermining respect for the law. One example arises from the PECR Regulations. These impose a clear obligation on organisations not to send unsolicited marketing faxes to individual subscribers who have not consented. Nevertheless there are businesses

that find this activity profitable and appear to be prepared to flout the law until they are prevented from doing so. With the possible exception of the enforcement powers available to the Commissioner under Part 8 of the Enterprise Act 2004, the enforcement tools available to the Commissioner are a cumbersome and ineffective way of addressing such deliberate and persistent misconduct.

Another example is inadequate security leading to the loss of personal data. It is well known that the Financial Services Authority (FSA) fined the Nationwide Building Society a sum approaching £1 million for failing to have effective systems and controls in place to manage its information security risk. This arose from the theft of a laptop containing confidential information on over 11 million customers. However financial information is not the only type of information that puts individuals at risk. Whilst the Information Commissioner is not seeking powers comparable to those available to the FSA it is a significant anomaly that no penalty at all would be available were an employer to similarly fail to manage the security of its HR records or a hospital or private clinic fail to manage the security of medical records.

This is relevant to the recent case at HMRC involving the loss of child benefit records. The Commissioner does not want to prejudge the outcome of the enquiry being undertaken by Kieran Poynter of PWC but even were that enquiry to find that HMRC had acted knowingly or recklessly in allowing an unprecedented security breach to take place he would have no powers to impose any penalty.

A New Penalty

Section 4(4) of the Act provides that, subject to some exemptions, -
"… it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller"

The Commissioner is proposing the introduction of a new penalty linked to this duty but limited to breaches that are avoidable, that give rise to a serious data protection risk and where a criminal state of mind exists. It would address behaviour that amounts to either a wilful disregard for the requirements of the Act or a grossly negligent approach to applying its requirements.

The precise form any penalty might take will require careful consideration. The creation of a new criminal offence is an obvious option but there might be other more effective alternatives. A suggested starting point for a new criminal offence is:-

1. *A data controller who, knowingly or recklessly, fails to discharge the duty imposed by section 4(4) is guilty of an offence where that failure results in a substantial risk that any person will suffer damage or distress.*

2. *It is a defence for a data controller charged with an offence under subsection (1) to prove that he exercised all due diligence to comply with the section 4(4) duty.*

For the avoidance of doubt the Commissioner wants to make clear that he is not seeking a custodial sentence for any new offence. The possibility of an unlimited fine

is the appropriate penalty. He is also open to the possibility that sanctions other than the power to bring a prosecution in the criminal courts might be appropriate. A civil penalty regime is one possibility and might have the advantage over a criminal penalty of being equally applicable to the Crown. The powers of the Financial Services Authority as set out in the Financial Services and Markets Act 2000 could provide a useful model to work from in the context of civil penalties. The Regulatory Enforcement and Sanctions Bill is also relevant. The intention of the Bill is to make available to designated regulators an "extended sanctioning toolkit". This "toolkit" includes fixed monetary penalties that can be imposed as an alternative to criminal prosecution where criminal offences exist. The Commissioner expressed reservations about the value of the "extended sanctioning toolkit" in the context of the criminal offences for which he can currently prosecute. Nevertheless he can see that were an offence to be introduced of the type suggested above the proposed "toolkit" could well provide added flexibility by enabling him not just to prosecute but to select the most appropriate and effective response to any particular instance of non compliance.

Existing Powers

The Commissioner has limited powers to make checks to ensure that the processing of personal data by organisations is being carried out in accordance with the Act's requirements. His existing powers fall into four main areas:

- Section 43 - Information notices. The power to serve a data controller with a notice requiring the data controller to provide the Commissioner with such information as is specified in the notice. A notice can be issued if the Commissioner has received a request for assessment or if he reasonably requires any information for determining whether a data controller is complying with the data protection principles.

- Schedule 9 - Powers of entry and inspection. The power to apply to a circuit judge for a search warrant where there are reasonable grounds for suspecting that a data controller is contravening any of the data protection principles, or that an offence has been committed and that evidence can be found on the premises in question.

- Section 51(7) - Assessment of good practice. The power, with the consent of the data controller, to assess any processing of personal data for the following of good practice.

- Section 54A - Inspection of overseas information system. The power to inspect any personal data recorded in certain overseas information systems for the purposes of assessing whether or not any processing of the data is being carried out in compliance with the Act.

The Commissioner uses and will continue to use all the powers available to him. However his powers do not include a general power to inspect personal data to ensure that the requirements of the law are being complied with. This power, insofar as it exists, is confined to certain overseas information systems. It was introduced as an amendment to the Act to give effect to the obligations on the UK arising from the

international agreements setting up the information systems in question. A wider ability to inspect the processing of personal data is important to the Commissioner. As explained in more detail below it is usual in any regulatory regime that those subject to regulation can be subject to inspection by the regulator. This provides an important incentive to regulated organisations to comply with the law. It also provides reassurance to the public that the regulation is effective in protecting their interest. Furthermore it gives the regulator opportunities to gain an insight into the practices adopted in the regulated sector.

Inspection is an important and growing aspect of the work of the ICO. It has for example been used to examine the processing of patient data by a sample of NHS Trusts. It has also been used to follow up undertakings given to the Commissioner in a number of areas including banking security. However, with the exception of overseas information systems, the ICO has to rely on the consent of the data controller concerned. This is both inappropriate and inefficient. The Commissioner would use any new power responsibly but the process of persuading data controllers to accept a voluntary inspection, negotiating the terms of an inspection, agreeing arrangements and then trying to hold a data controller to them can be difficult and time consuming. The Commissioner, whilst being careful not to compromise his statutory duty, has had to give assurances to data controllers in return for their cooperation, that limit any follow up action that he might take. Although he has concluded that it is preferable to undertake an inspection with limitations rather than not undertake an inspection at all, he does not consider that it is helpful either in terms of providing reassurance to the public or in providing an incentive for compliance that he has to compromise the discretion he would otherwise have over the scope of his inspections or any follow up regulatory action that might be appropriate in the circumstances.

Although the Commissioner's staff are inclined not to waste effort by pursuing reluctant data controllers to the point of a firm refusal there is some evidence, particularly from the private sector that whilst more junior data protection staff can see the value in a voluntary inspection it is looked on as an avoidable business risk once the decision moves to a higher level. In at least one instance an initial invitation to the ICO to conduct an inspection, involving the use of overseas call centres, was subsequently withdrawn. There have also been examples in the public sector. In one case the data protection officer from a university approached the ICO about conducting an inspection. However after protracted correspondence, but no outright refusal, it became clear that senior management reservations were effectively blocking progress. In another case an NHS trust approached the ICO for an inspection. After the first stage of the inspection had been completed the trust refused to let the second stage go ahead. The resources devoted to both arranging the inspection and completing the first stage were therefore largely wasted.

Another situation where the Commissioner would wish to use an inspection power is where the extent of non-compliance and any consequent enforcement action that might be needed is unclear. One example arose with a supplier of telecommunications services. Over 70 complaints were received about the organisation on a variety of issues. These suggested a systemic problem in the organisation's approach to managing its data protection obligations. The ICO wished to undertake an inspection to establish the nature and extent of this problem and

hence what remedial action might be required. Although the organisation concerned agreed that an inspection was an appropriate way forward it never proved possible to pin them down even though complaints were continuing.

The Commissioner does have the power to obtain a search warrant in connection with breaches of the data protection principles. He is considering whether this power might be more widely used but does not believe that it is a suitable alternative to a general inspection power. A search warrant can only be obtained where there are reasonable grounds for suspecting a breach. Whilst a risk-based approach will be taken to the use of any general inspection power it is important that checks can be made on any processing of personal data before the stage where harm has been caused.

Furthermore the formality of the process of obtaining a search warrant is inevitably a confrontational one. It is likely to cause alarm to a responsible data controller. The process is seen as heavy handed with stigma for those involved. There would probably be a strong adverse reaction if search warrants were to be much more widely used. This conflicts with the Commissioner's approach to inspection which he wishes to promote as a primarily constructive exercise, preferably involving the active participation of the data controller's staff and providing practical benefits to the data controller.

New Inspection Powers

The Commissioner is seeking a new inspection power based on the current section 54A of the Act but not limited to overseas information systems. The power might be framed by amending section 54A along the following lines:

Inspection of information systems

1. *The Commissioner may inspect any personal data recorded in any information system which he has reason to believe is used or intended to be used for the processing of personal data.*

2. *The power conferred by subsection (1) is exercisable only for the purpose of assessing whether or not any processing of the data has been or is being carried out in compliance with this Act.*

3. *The power includes power to inspect, operate and test equipment which is used for the processing of personal data and power to examine policies, procedures and records relating to the processing of personal data.*

4. *Before exercising the power, the Commissioner must give notice in writing of his intention to do so to the data controller.*

5. *Subsection (4) does not apply if the Commissioner considers that the case is one of urgency.*

6. Any person who -

(a) intentionally obstructs a person exercising the power conferred by subsection (1), or

(b) fails without reasonable excuse to give any person exercising the power any assistance he may reasonably require,

is guilty of an offence.

The Commissioner can give an assurance that any new powers will be used in accordance with good regulatory practice. He is on the point of publishing his Data Protection Strategy and will concentrate any inspection activity on those organisations and those forms of processing that give rise to the greatest data protection risk. A new power would not change his commitment to "making it easier for the majority of organisations who seek to handle personal information well …". In practice an inspection power could be a way of encouraging enlightened self regulation perhaps through the Commissioner giving an assurance to those who are awarded a data protection "seal" by an accredited body that they would not normally expect to face an inspection by the Commissioner's staff.

Developments in EU legislation are placing requirements on the ICO that are difficult if not impossible to meet without an inspection power. The Data Retention (EC Directive) Regulations 2007 place the Information Commissioner under a duty to monitor the application of the Regulations with respect to the security of stored data. The Commissioner will be unable to properly discharge this duty without a power that gives him the right to inspect the security arrangements made by service providers. Furthermore the Prüm Convention, which is to be incorporated into the EU legal framework, places an obligation on data protection authorities to carry out random checks on the lawfulness of the supply of personal data. It also requires data protection authorities to "perform the inspection tasks necessary for mutual cooperation". Without an appropriate inspection power the Commissioner will be unable to meet these obligations that he expects to be placed on him.

It is also well known that the European Commission has been examining the compatibility of UK legislation with the requirements of Directive 95/46/EC. One area that the Commission has particularly focussed on is the powers of the Information Commissioner. Whilst the Commissioner would not claim that there is an incontestable case that the Directive requires him to have a compulsory inspection power the Directive does require that each supervisory authority has "investigative powers such as powers of access to data forming the subject matter of processing operations and power to collect all the information necessary for the performance of its supervisory duties". Extending the Commissioner's powers would place beyond doubt the question of whether the UK has properly implemented this aspect of the EU Directive.

Coupled with a new inspection power is the proposal that the Information Commissioner should have a power to require a data controller to provide him with a report by a skilled person. This is based on the power given to the Financial

Services Authority in section 166 of the Financial Services and Markets Act 2000. It would be used, in particular, where there are grounds to believe that there has been or could be a significant breach of the Act's requirements and technical expertise is needed to determine whether this is the case and if so what remedial action might be appropriate. This is most likely to arise in the context of security breaches.

An example is the recent breach of security on a visa application website operated by the Foreign and Commonwealth Office (FCO). Given the technical nature of the security breach the FCO commissioned their own expert report and agreed to provide the ICO with a copy. They have subsequently provided the Information Commissioner with a formal undertaking based on the recommendations in the report. Although the FCO voluntarily commissioned an expert report there is no guarantee that another data controller would do so in similar circumstances in the future. Whilst the ICO could, if it is given the inspection powers referred to above, commission its own expert report there is a strong argument that the obligation to do so and the costs involved should fall on the data controller concerned.

Enhanced Enforcement Powers

The ICO's experience of exercising the enforcement powers in the Act has led the Information Commissioner to conclude that they are cumbersome and ineffective in addressing the most serious cases of deliberate and persistent misconduct. Reference has already been made to the difficulty of enforcing the Act against those who choose to ignore its requirements. In some cases this could have serious consequences and the conduct that is in breach needs to be brought to an immediate halt. An example would be where, because of inadequate security, personal information is mislaid by a data controller and falls into the hands of a third party. The third party might have acquired the information innocently but then sets out to misuse it. This could happen, for example if a data controller mistakenly sends personal data either on disks or electronically to an unintended recipient.

In addition to calling for a new penalty to address this the ICO would welcome injunctive powers of intervention that would effectively stop the unlawful practices from continuing pending any prosecution or other enforcement activity. At present, following service of an enforcement notice (under section 40 of the Act) to address a breach of principle, that notice can be appealed to the Information Tribunal and pending the determination of that appeal the effect of the notice is suspended (see section 40(7) of the Act). It can take many months for an appeal to be heard and a determined data controller can deliberately delay progress.

Section 40(8) of the Act makes specific provision for an urgency statement to be endorsed on the notice where the Commissioner adjudges there to be "special circumstances". The inclusion of such statement can be appealed to the Information Tribunal (see section 48(3)). Only once any such appeal is determined (and only then if the appeal is dismissed) will the inclusion of an urgency statement have the effect of requiring compliance with the notice pending any substantive appeal against the notice. Any notice including an urgency statement does not have to be complied with during the seven day period after service within which the data controller can appeal against the inclusion of the statement. As such, the Commissioner does not have an effective injunctive power to stop immediately the most serious breaches –

including breaches which, if the new offence suggested earlier becomes law, would be criminal breaches.

To address this the Commissioner seeks such injunctive powers, either by way of an adaptation of the provisions of section 40, or by way of additional powers. In either case it is suggested that such powers might be modelled on the Part 8 Enterprise Act powers which provide for enforcement orders and interim enforcement orders. The Information Commissioner recognises that the scope of the Enterprise Act does not extend beyond the business community whereas any new enforcement powers would need to be exercisable against all data controllers. The Commissioner also recognises that the procedure would need to be more streamlined than that under the Enterprise Act 2002 in that it should not include prior reference to another enforcement body (such as the OFT in the Enterprise Act). Any such prior approval, other than through the Courts, would compromise the Commissioner's independence as the UK supervisory authority for data protection.

In addition, the Commissioner would welcome the specific inclusion of undertakings (as provided for in the Enterprise Act enforcement regime) as a regulatory outcome in connection with the exercise of enforcement powers. This route is already pursued on a non-statutory basis in the exercise of the Commissioner's existing enforcement powers. In this context it is relevant to refer again to the Commissioner's response to the Regulatory and Enforcement Sanctions Bill consultation. His response to the proposal contained in clause 34 of that draft legislation, for the availability of "enforcement undertakings" to designated regulators (including the Commissioner) is relevant in this context. He recognised that such provisions would merely place on a statutory footing a regulatory tool that the ICO has used to date quite effectively on a non-statutory basis. The proposals in that Bill for an extended sanctioning toolkit to be available to designated regulators were built on the premise that the additional sanctions available would all be alternatives to prosecution for criminal offences but some provisions, including enforcement undertakings, could have a role in their own right.

There is a further weakness in the Commissioner's enforcement powers that needs to be addressed. This is that enforcement notices can only be served if the Commissioner is satisfied that a data controller "has contravened or is contravening" any of the data protection principles. There are occasions when the Commissioner becomes aware that a data controller is likely to contravene the data protection principles but has not yet done so. This can occur where a data controller seeks advice from the ICO on a proposal for processing personal data but then declines to follow the advice given. There is an unnecessary and avoidable risk created for individuals by preventing the Information Commissioner from intervening until a breach and any associated damage or distress to individuals, has actually occurred. this risk could be removed by extending the basis on which an enforcement notice can be served to include circumstances where the Commissioner is satisfied that a data controller "is likely to contravene" any of the data protection principles.

The Information Commissioner believes that an overhaul of the enforcement powers available to him is overdue. Whilst the draconian nature of an effective injunctive power militates against its use in all but the most serious of cases – more than likely cases involving criminal or similar liability as well – the Commissioner would not want

it restricted to commission of offences. This would also be the case for the use of non-injunctive enforcement powers, including undertakings, which should be available for any breach of principle that warrants the use of such powers in accordance with the ICO's Data Protection and Regulatory Action Strategies.

Extended Information Notice Power

Currently the Commissioner's information notice power under the DPA only enables him to require information from the data controller. He has some information gathering powers under the Regulation of Investigating Powers Act but these can only be used in the investigation of criminal offences. These are circumstances where he needs to obtain information from someone other than the data controller in order to investigate non-criminal data protection breaches. This happens most commonly in relation to PECR breaches, where it may be necessary to identify who the subscriber to a particular phone or fax number is, or who is 'behind' an e-mail address or website. Typically it is the provider of the relevant telecommunications service who holds this information. Without the necessary information it can prove impossible either to identify the sender of an offending message or to tie an offending message evidentially to a particular sender.

This defect in the information notice power could be rectified by changing references to "the data controller" to "any person" in section 43 of the Act.

The Increasing Risks

This case for amending the Data Protection Act is made against a background of ever-increasing collection, use and sharing of personal information. This brings benefits, such as more efficient delivery of services and more effective detection of crime, but it also brings risks. These include the risk that individuals suffer harm because information about them is

- inaccurate, insufficient or out of date
- excessive or irrelevant
- kept for too long
- disclosed to those who ought not to have it
- used in unacceptable or unexpected ways beyond their control
- not kept securely.

There is also a risk of wider societal harm that might for example arise from the negative aspects of a surveillance society.

Data protection law was originally introduced in the UK in 1984 to counter the risks posed by the development of computerised information systems. With limited exceptions, most particularly the section 55 offences, the powers and penalties available to the Information Commissioner remain little changed from those available

to the original Data Protection Registrar under the 1984 Act. Since 1984 the growth in processing of personal information has been phenomenal. Alongside this the risks have also increased. It is important that the safeguards that are provided through the Act, including the powers and penalties available to the Commissioner, are updated to match the growth in risk.

The Government itself is committed to more information sharing to deliver better public services. In her foreword to the Government's "Information sharing vision statement" Baroness Ashton said that "… the more we share information, the more important it is that people are confident that their personal data is kept safe and secure". Public trust and confidence in the handling of personal information are key to the success of private as well as public sector organisations. Providing the Information Commissioner with regulatory tools that are up to the challenges he now faces is an important element of building and maintaining this trust and confidence that responsible organisations increasingly depend on.

The importance of updating data protection powers and penalties is reflected in the Report of the House of Lords Science and Technology Committee on Personal Internet Security (Aug 07). In its conclusions and recommendations the Committee states, at para 5.57, that:

> *"We further recommend that the Government examine as a matter of urgency the effectiveness of the Information Commissioner's Office in enforcing good standards of data protection across the business community. The Commissioner is currently handicapped in his work by lack of resources; a cumbersome "two strike" enforcement process; and inadequate penalties upon conviction. The Government have expressed readiness to address the question of penalties for one type of offence; we recommend that they reconsider the tariffs for the whole of the data protection regime, whilst also addressing resources and enforcement procedures as well. These should include the power to conduct random audits of the security measures in place in businesses and other organisations holding personal data."*

The House of Commons Home Affairs Committee and the House of Lords Constitution Committee are both conducting inquiries on matters related to the surveillance society and data collection. It is not possible to predict the outcome of these inquiries. However both committees have already expressed interest in whether the current provisions of the Act provide sufficient safeguards in the climate of ever increasing surveillance of individual citizens.

Better Regulation

It would be easy to suppose that any increase in data protection regulatory powers and penalties should be resisted on the grounds that it is increased "red tape" and imposes a burden on business. This would be mistaken. An increase in powers and penalties is not of itself an increase in regulation. It merely helps ensure that the existing regulation is properly complied with. This "levelling of the playing field" is in the interests of the majority of organisations who seek to handle personal information well and should be welcomed. There would of course be some burden

for the small number of organisations chosen for inspection which, under the present voluntary arrangement might refuse. Here the Commissioner will ensure that any burden is concentrated on organisations and processing that pose the greatest data protection risk.

A great deal of attention has been paid recently to the importance of "better regulation". This includes the Hampton Report on "Reducing administrative burdens: effective inspection and enforcement" and the Macrory Report on "Regulatory Justice: Making Sanctions Effective". In both these reports the emphasis is not on keeping sanctions to a minimum. It is on having effective sanctions available to regulators and on the sanctions being used proportionately. This is entirely in line with the Information Commissioner's aims. More specifically the Hampton Report, when addressing the control of illegal activity, states:

> "2.72 Effective control of this illegal activity is important for regulators and businesses alike. It is important for regulators, as a way of improving the outcomes of the regulations they enforce. It is important for businesses because illegal operators can undercut legitimate businesses, often by quite considerable sums.
>
> 2.73 The penalty regime should aim to have an effective deterrent effect on those contemplating illegal activity. Lower penalties result in weak deterrents, and can even leave businesses with a commercial benefit from illegal activity. Lower penalties also require regulators to carry out more inspection, because there are greater incentives for companies to break the law if they think they can escape the regulator's attention. Higher penalties can, to some extent, improve compliance and reduce the number of inspections required."

This theme of appropriate rather than minimum penalties is taken forward in the UK's programme of regulatory reform set out by the Government in "Next Steps on Regulatory Reform" (July 2007). This programme includes several elements, one of which is

"Ensuring that regulators have access to a flexible set of modern sanctioning tools that are consistent with the risk-based approach to enforcement outlined by Philip Hampton".

Turning to regulatory inspections there is a great deal of emphasis in the Hampton Report on the carrying out of inspections and on any burden they impose, being concentrated on areas of greatest regulatory risk. This is an approach that the Information Commissioner wholeheartedly endorses. However the Hampton Report does not directly address the question of whether regulators should have a power of compulsory inspection. Hampton starts from the position that such a power exists and then examines how the power should be used. His presumption appears to be that in any regulatory system with an independent regulator that regulator will have an inspection or similar power to ensure that the relevant regulations are complied with in practice. This is clearly the case in the particular regulatory systems that Hampton investigated.

Other Regulators

Some comparative information on the powers and penalties available to other UK regulators is attached at Annexe 1 and on the powers and penalties available to other European data protection authorities at Annexe 2. The Commissioner recognises that it is difficult to draw precise comparisons. Other UK regulators are not enforcing data protection legislation and other EU authorities operate within different legal systems and cultures. Nevertheless some important points emerge:

- the power to carry out inspections of those regulated without necessarily having the permission of the organisation concerned is available to most, if not all, other data protection authorities in the EU. It is also commonplace amongst other UK regulators.

- a good comparator is the Health & Safety Executive (HSE) which is similar to the ICO in that it enforces legislation based on a duty to comply with broad principles of good practice that are universally applicable to organisations whether in the public or private sectors. There is a general criminal offence, prosecuted by the HSE, where a person fails to discharge this duty. The HSE and other enforcing authorities appoint inspectors who have a power to carry out inspections at any reasonable time.

- another important comparator is the Office of Communications (OFCOM). They have the power to issue a penalty of up to £50,000 following a procedure which is similar in some ways to the process followed by the ICO when issuing an enforcement notice. Where there are reasonable grounds for believing that a person has persistently misused an electronic communications network or service OFCOM can give that person a notification. If the persistent misuse continues they can impose a penalty that is appropriate and proportionate to the misuse, having due regard to any representations made or remedial action taken by the misuser.

ANNEXE 1

POWERS AND PENALTIES AVAILABLE TO SOME UK REGULATORS

Health and Safety Executive

Legislation: Health and Safety at Work etc Act 1974, 31 July 1974 – amended and modified several times

Sanctions

HSE can serve a statutory improvement notice or, where there is a risk of serious personal injury, a statutory prohibition notice. These notices apply to the private and public sectors but not to Crown bodies.

For Crown bodies, they can serve a Crown notice. Crown notices are similar but are not legally binding and the Crown cannot be prosecuted for a breach of these notices.

HSE can, in appropriate cases, prosecute without prior warning or recourse to alternative sanctions. Again Crown bodies can not be prosecuted but they can be subject to formal censure.

HSE can also withdraw approvals, vary licence conditions or exemptions and issue formal cautions.

Failing to comply with an improvement or prohibition notice is punishable by the courts. The maximum penalty in the lower court is £20,000 and/or 6 months' imprisonment. In the higher court, the maximum penalty is an unlimited fine and/or 2 years' imprisonment. The same financial penalties apply to breaches of sections 2-6 of HSWA, which set out the general duties of employers, self-employed persons, manufacturers and suppliers to safeguard the health and safety of workers and members of the public who may be affected by work activities. Other breaches of HSWA and breaches of all health and safety regulations are punishable by fines of up to £5,000 in the lower court or unlimited fines in the higher court.

Audit/Inspection

Under section 20 of HSWA, HSE can enter and inspect premises without notice or permission for the purpose of carrying into effect any of their relevant statutory provisions. They can inspect and take copies of documents and interview members of staff.

HSE use their inspection powers where they have evidence that health and safety is poor, where they are dealing with certain hazardous industries or where they want to investigate a specific incident or complaint. They also carry out a limited number of inspections to make an assessment of the risks in new businesses or premises, to target certain geographical areas or sectors usually to concentrate on specific

priorities, to do random ‘spot checks’ on compliance or to keep abreast of new developments and processes or for training purposes.

They no longer collect or publish figures relating to the number of inspections. However, in 2002/3 (the latest year for which figures are available), they carried out 84,234 inspections.

Financial Services Authority

Legislation: Financial Services and Markets Act 2000, 14 June 2000 – amended several times

Sanctions

The FSA can impose various sanctions. These include withdrawing a firm’s authorisation, disciplining authorised firms and people approved by the FSA to work in those firms, imposing financial penalties, applying to the court for injunction and restitution orders and prosecuting various offences.

In 2006/7, the FSA imposed 32 financial penalties totalling £14,661,143. This included a fine of £6,363,643 on Deutsche Bank AG for failing to observe proper standards of market conduct and failing to conduct their business with due skill, care and diligence. They also imposed a financial penalty of £350,000 on Deutsche Bank’s former Head of European Cash Trading for being knowingly concerned in the misconduct which resulted in the breaches.

If a person has breached a relevant requirement under FSMA and profits have been generated or loss caused because of the breach, the FSA can apply to the court for a restitution order. If they are successful, the court can order that person to repay any profits and compensate victims for any loss.

The FSA can prosecute several offences. These cover a range of misconduct including falsely claiming to be FSA authorised, carrying on a regulated activity without authorisation, making misleading statements to induce investments and failing to co-operate with FSA investigations. Some of the offences are punishable by a fine; others carry a maximum of 7 years’ imprisonment.

Audit/Inspection

The FSA has extensive statutory powers of investigation, including powers to require the production of documents and to require certain persons to attend interviews. If someone does not attend an interview required under FSMA he can be dealt with by the court as if he were in contempt (where the penalties can be a fine, imprisonment or both).

In certain circumstances, the FSA can apply to the court for a search warrant.

The FSA also has a power, under section 166 of FSMA, to require a firm and certain other persons to provide a report by a skilled person. The FSA may use this power

to require reports by skilled persons to support both their supervision and enforcement functions.

Ofcom

Legislation: Communications Act 2003, 17 July 2003 – amended and modified several times

Sanctions

Where Ofcom has reasonable grounds for believing that a person has persistently misused an electronic communications network or service, they can issue a notification under section 128 of the Act which sets out their views and gives the person the opportunity to make representations.

If the misuse continues, they can issue an enforcement notification under section 129. This requires the person to take steps to cease the misuse, avoid its repetition and remedy its consequences. The required remedial action may involve the payment of compensation to persons who have suffered loss or damage, or annoyance, inconvenience or anxiety as a result of the misuse.

If a person fails to comply with an enforcement notification, Ofcom can bring civil proceedings for an injunction, for specific performance of a statutory duty or for any other appropriate remedy or relief.

As an addition or an alternative to an enforcement notification, Ofcom can impose a financial penalty under section 130. The maximum financial penalty for persistent misuse was increased on 6 April 2006 from £5,000 to £50,000 (SI2006/1032).

They can also issue notifications and enforcement notifications to communications providers under sections 94 and 95 of the Act for breaches of the General Conditions (21 enforceable obligations and standards for communications providers). If a communications provider continues to breach the General Conditions after receiving a notification and enforcement notification, they can be fined up to 10% of their turnover.

In 2006/7, Ofcom imposed 8 financial penalties totalling £422,000. The largest fine imposed was in excess of £100,000.

Audit/Inspection

Ofcom does not have specific audit or inspection powers under the Communications Act but does have the power to investigate anti-competitive behaviour.

Office of Fair Trading

Legislation: Competition Act 1998 (9 November 1998), Consumer Credit Act 1974 (31 July 1974), Enterprise Act 2002 (7 November 2002)

Sanctions

Competition Act: Businesses that breach the Act can be fined up to 10% of their annual worldwide turnover. In addition, individuals found to be involved in cartels can be fined and imprisoned for up to 5 years and directors of companies that breach the prohibitions can be disqualified for up to 15 years.

Consumer Credit Act: The Act requires most businesses that offer goods or services on credit or lend money to consumers to be licensed by the OFT. Trading without a licence is a criminal offence and can result in a fine or up to 2 years' imprisonment. The OFT has the power to refuse, suspend or revoke licences.

Enterprise Act: The OFT can seek an undertaking or apply to the court for an enforcement order. Failure to comply with an enforcement order could be found by a court to be contempt of court, which could lead to a fine or imprisonment.

Audit/Inspection

Competition Act: The OFT has a wide range of powers to investigate suspected infringements. They can obtain documents and information from businesses suspected of committing an infringement as well as from their competitors, customers or suppliers. They can also enter, and where they have obtained a warrant, search premises. Anyone who fails to co-operate with the investigation, obstructs OFT officials or hides, destroys or falsifies relevant documents may be guilty of a criminal offence punishable by a fine and/or, in some cases, imprisonment. In 2006/7 the OFT visited 14 premises using their formal civil investigatory powers under the Competition Act. They also visited 4 premises under criminal search warrants obtained under section 194 of the Enterprise Act.

Consumer Credit Act: The OFT has powers of entry and inspection under section 162 of the Act. They can also apply for warrant if admission is likely to be refused. In 2006/7, 16 applications were made seeking the OFT's authorisation under section 162 of the Act to use powers of entry and inspection.

Enterprise Act: Under Part 8 of the Act, as amended by the Enterprise Act 2002 (Amendment) Regulations 2006, the OFT has the power to gain access to premises without a warrant, to require persons to produce goods or documents and to give an explanation about such goods or documents, to seize goods or documents for certain purposes and to enter and search premises under a warrant. The OFT can exercise its on-site inspection powers if there is a reasonable suspicion that an infringement has been committed or is likely to be committed or to investigate whether a person has complied with or is complying with an undertaking or enforcement order. In order to enter premises without a warrant, the OFT must give the occupier of the premises at least 2 working days' written notice.

ANNEXE 2

POWERS AND PENALTIES AVAILABLE TO SOME EU DATA PROTECTION AUTHORITIES

Denmark

Legislation: Act on Processing of Personal Data, 1 July 2000 - amended several times, most recently 1 July 2007

Any person or legal entity committing an offence - fine or imprisonment
DPA cannot impose sanctions; they request the Danish Public Prosecution Office to instigate proceedings.
Highest fine to date: £2,500
No prison sentences to date.

The DPA can issue an enforcement notice or go straight to an offence and pass the case to the public prosecutor. It depends on the case. This is for private sector only.

For the public sector, they inform the relevant minister or head of the municipality. They cannot fine or give prison sentences to public authorities.

Once a case is with the public prosecutor it becomes like any other criminal case, and the court decides on the fine and or other sanctions.

Audit/Inspection

The DPA can audit public or private sector organisations without notifying them in advance and they don't need the organisation's permission.

The DPA can only audit private sector organisations where they are processing as covered by s50 of their law (the organisation is notified or they are processing data they need an authorisation for.

Generally, the DPA do inform the organisation in advance of an audit / inspection by sending a letter, and they usually ask for information in advance of the audit, such as the security description.

If there are problems found, they ask the company to send them any information / notify and so on. When the DPA is satisfied, they send a final letter to sum up the case and close it. They sometimes have to notify the police if they find serious problems during the inspection.

The DPA reports to Parliament every year and this includes the number of inspections done. Their target is 60 a year and they average 60 to 70.

Ireland

Legislation: Data Protection Act 1988, modified by Data Protection (Amendment) Act 2003

1 July 2003

Breaches may incur civil liability or criminal sanctions, including fines.
Blagging offence - €3,000 - not prosecuted anyone yet
Failure to comply with notices - €3,000
Prosecution on indictment - up to €100,000 - never used yet, not clear under what circumstances it could be used. Possibly for complete failure to respond at all, or actions affecting a lot of people.
No prison sanctions
Breach of principle is not an offence, may result in enforcement notice.

The DPA has the same powers as the ICO in terms of serving information and enforcement notices. They also have a prohibition notice relating to international transfers.

Audit/inspection

They have the power under s10 of their law to audit for practice and compliance with the Act. They don't tend to use this power. In they do, they contact the company and tell them they will audit on a particular date. The company has some leeway to change the date, but not much.

Instead they use (and increasingly so) the power under s24 to be able to enter any premises at any time without notice. It is a power of entry and to copy information. They can turn up anywhere at any time and look at personal data processed or information relating to the processing. A failure by an organisation to cooperate is an offence and they are cautioned and possibly prosecuted. They do not take the police with them, it has not been needed so far, but they could ask if they wanted to.

They are increasingly using this power with organisations involved in mobile marketing. Under the legislation that has enacted the e-privacy directive they have the power to prosecute any offences under that law and to impose fines of €3,000 for every message sent or every failure to comply. The court can also order the deletion of a database and there is draft legislation at the moment to increase the fine to €5,000; and a maximum of 10% of a company's turnover, or €4 million. Some large-scale prosecutions are expected.

The Director of public prosecutions carries out the sanctions. The DPA makes the case and takes it to court. They recommend the fine or other sanction (measures to be taken and so on). The court decides ultimately, and may levy fines of less than the DPA recommends. For example, €500 per message rather then €3,000.

The DPA aims for 30 audits per year.

Italy

Legislation: Protection of individuals and other subjects with regard to the processing of personal data Act - replaced by the Consolidation Act regarding the processing of personal data

8 May 1997 / 1 Jan 2004

Criminal, civil and administrative sanctions

Can impose admin sanctions - fines - for not providing data subject with info subject to information notice or for non-notification
Up to 3 years in prison and publication of judgement for unlawful processing, if damage occurs; false notification; and failure to adopt and implement the required security measures.

The DPA put together a case and if there is evidence of criminal conduct, they pass the information on to the police and judicial authorities. The judicial authorities carry out any investigations. They can then impose sanctions including up to 3 years in prison, as described above.

The DPA can ask an organisation for information and documents and the organisation has to reply. If they don't, they are liable to a fine or criminal punishment. Fines are from €4,000 to €24,000. Criminal punishments are used for repeat offenders or for providing false information. The DPA can issue the order to pay a fine.

Audit/Inspection

The DPA targets organisations or sectors based on intelligence from complaints or by acting on their own initiative and according to their priorities. If these paper inspections do not yield enough information, they can carry out on the spot inspections.

These inspections can be 'dawn raids', but usually they give advance notice of an inspection, but do not say what they are looking for.

They have an MoU with the financial police who can carry out inspections across Italy based on established questions and following the Garante's instructions. There is a special squad to deal with dp cases and they have had training from the Garante and are familiar with the dp law and requirements. This allows the Garante to cover the country. If it is a complex case there may be someone there from the Garante as well.

A report is done on site and signed by all present. The final decision on the case is published on the website.

The DPA also uses name and shame tactics and can impose lower sanctions if the organisation has co-operated.

In 2006 they carried out 350 inspections with 158 administrative breaches found and 11 cases referred to the judiciary.

France

Legislation: 2004-801 law of 6 August 2004, recently amended.
Sanctions available: warnings, formal demands, injunction to cease processing, financial sanctions up to €150,000 for first breach and up to €300,000 for further breaches. Criminal sanctions up to max 5 years in prison and fines from €15,000 to €300,000.

The CNIL can issue warnings and compliance notices (like enforcement notices). Non-compliance with these can result in financial sanctions (but not the public sector) of up to €150,000, then up to €300,000 for subsequent offences, or 5% of turnover - up to a max of €300,000. Or they can issue an order to stop processing. Fines only follow the issuing of a notice.

Serious cases can be referred to the public prosecutor, although this rarely happens. It is usually in cases where the CNIL does not have the power to carry out the necessary investigations. The courts can issue fines or prison terms - up to 5 years in prison and fines of up to €300,000.

In emergency cases they can interrupt or block processing for up to 3 months, or inform the Prime Minister if public security files are involved. The President can ask a judge to order any necessary security measures in serious cases. They can also withdraw their authorisation.

Audit/Inspection

The DPA can access all professional premises, request and copy all necessary documents, access all IT systems, and request transcriptions of data.

They used to inform companies of inspections but this didn't work very well, so now most are on-the-spot inspections. They have to inform the local judge in case they are refused access to premises, in which case the judge can order the company to let them in.

Non-compliance with report recommendations can lead to the threat of financial sanctions, or they can refer the case to the public prosecutor.

In 2006 they carried out 127 inspections.

Spain

Legislation: Ley orgánica 15/1999
14 January 2000

The Agencia Espanola De Proteccion de Datos (AEPD) has supervisory responsibilities for all issues related to the protection of personal information in the private sector and public sector (except local public sector in Madrid, Cataluna and the Basque Country.

Because the agency has the power to impose sanctions, it must guarantee due process to all parties. In this respect they have a number of powers available to them. They are able to:

(i) Request that the data controller under investigation voluntarily submits information.
(ii) Inspect organisations in situ – failure to assist the Agency is a serious infringement.
(iii) The Agency may lawfully impose fines on the data controller (private sector only) if violations in respect of the data protection legislation are discovered.
(iv) As a preventative measure they may block or stop processing of personal information.

Sanctions (fines) may be imposed following inspection and investigation. Sanctions are imposed in accordance with a sliding scale dependent upon the seriousness of the infringement. Very serious violations may incur fines up to 600,000 Euros. Examples of very serious violations are:

(i) Unauthorised transfer of data.
(ii) Unauthorised processing of specially protected data (medical, racial, sexual, ideological)
(iii) Fraudulent collection of data.
(iv) Systematic violations.

Serious violations may incur fines of up to 300,000 Euros. Examples of serious violations are as follows:

(i) Failure to maintain accuracy.
(ii) Failure to provide security measures.
(iii) Failure to register or notify as required.
(iv) Creation of data files without consent.
(v) Active refusal of rights.
(vi) Obstruction of investigation.

Audit/Inspection

The AEPD have the power to inspect/ audit without the consent of the data controller. Failure to collaborate in an inspection is a serious violation which may lead to a fine being imposed of up to 300,000 Euros.

In the case of infringement of data protection law by public sector organisations fines are not imposed but public warning are issued which may lead to disciplinary proceedings against individuals.

Investigations/audits carried out in 2006 –

1282 enforcement investigations started of which:

281 led to penal sanctions legal proceedings,
103 led to a public warning against public administration bodies