

Information Commissioner's Office

A Hampton Implementation Review Report

November 2009

Information Commissioner's Office

This review is one of a series of reviews of regulatory bodies focusing on the assessment of regulatory performance against the Hampton principles and Macrory characteristics of effective inspection and enforcement. It was carried out by a review team drawn from the Better Regulation Executive, from the Medicines & Healthcare products Regulatory Agency and the Gangmasters Licensing Authority, in April 2009.

Further information about the reviews can be found at:

<http://www.berr.gov.uk/whatwedo/bre/inspection-enforcement/implementingprinciples/reviewing-regulators/page44054.html>

EXECUTIVE SUMMARY AND CONCLUSIONS

Key findings from the review:

The review team found that the activities of the Information Commissioner's Office (ICO) were by and large compliant with Hampton principles in many areas. However, there are improvements that can easily be made, some of which will be more important as the ICO's resources increase. The review team noted that the direction of travel had been positive in recent years and that further steps were already being taken to operate in more Hampton-compliant ways in some of the areas of comparative weakness.

In addition to the key findings and main issues for follow up that follow, the review team has also made a number of other recommendations in this report that it considers the ICO should implement.

Key findings were:

- The ICO is taking a leading role on Data Protection issues within EU fora and is showing impressive strategic leadership on the topic of data protection.
- The ICO has a good working relationship with its major stakeholders; however, the review team believes that it would benefit from developing a more structured approach to stakeholder engagement.
- The ICO produces extensive, clear and accessible guidance for businesses and the public that is targeted at a number of levels (technical/general). It does so by working proactively and constructively with its stakeholders. The review team commends the approach being taken now to develop a 'meta-guidance' document.
- The ICO is a generally accessible organisation to stakeholders – both its website and helpline appear to be working well. However, there are inevitably improvements that can be made. In particular, the ICO should consider increasing resources and training for helpline staff, developing the effectiveness of its 'triage' system and further improving the structure and search facility of its website.

Main issues for follow-up identified during the review:

The key follow up issues identified during the review were:

- The relationship between the ICO and the Ministry of Justice (MOJ) appears to be less effective than it could be. It is critical that clarity about policy objectives and the mechanisms for delivering them is achieved on both sides, especially, and very promptly, in respect of the current legislative opportunity for the ICO to obtain new powers. In particular, ICO could be more proactive in producing effective, well-evidenced business cases to support the development of policy proposals – but it is also important that the MOJ ensures it fully understands the ICO's detailed rationale for its perceived business needs. The review team believes that would help lead to a more constructive and mutually productive relationship.
- The ICO is aware of the need to be risk-based in its audit/inspection approach, but currently it does not have documented or systematic processes for this. The review team considers this will become increasingly important as the ICO's audit function grows.
- In addition to the imminent new power to impose financial sanctions, the ICO could give greater consideration to making use of other elements of the expanded range of sanctioning options that will be available under the Regulatory Enforcement and Sanctions Act 2008.
- The ICO should articulate more clearly the outcomes that it is seeking to achieve and obtain appropriate publicity for its often excellent outcomes – both strategic and casework. In each case, it should address both its stakeholders and a wider public audience.

INTRODUCTION

Introductory background information about the regulator such as the rationale for establishing it:

The Information Commissioner's Office (ICO) was established on 30 January 2001 as a non-departmental public body (NDPB) sponsored by the Ministry of Justice (formerly the Department for Constitutional Affairs¹). The ICO's mission is to "Promote public access to official information and protect personal information".

The ICO's main functions are:

- the promotion of good practice – providing information and advice;
- the resolution of problems – addressing complaints from people who feel their rights have been breached; and
- enforcement – using legal sanctions to ensure compliance with data protection obligations.

Hampton Implementation Reviews focus on regulators' interaction with and impact on business. Because the responsibilities of the ICO under Freedom of Information legislation relate almost exclusively to public bodies, this review focuses on the regulatory activities of the ICO under data protection legislation.

The legislation establishing the regulator:

The origins of the Information Commissioner's Office lie in the Data Protection Act 1984. The Act introduced eight principles of good practice for the handling of data (the 'data protection principles'), with which data handlers are required to comply. A new body, the Data Protection Registrar, was created to administer a register of all people and companies processing personal data.

The next major legislative development in this area was Directive 95/46/EC of the European Parliament and of the Council of Ministers of 24 October 1995 (known as the 'Data Protection Directive').

The Data Protection Act 1998 (DPA) replaced the Data Protection Act 1984 and transposed the Data Protection Directive into UK law. The DPA regulates

¹ The Ministry of Justice replaced the Department for Constitutional Affairs on 09 May 2007.

the collection, use, distribution, retention and destruction of personal data. Following implementation of the Data Protection Act 1998 on 1 March 2000, the title of the office was changed to Data Protection Commissioner (DPC).

Following the introduction of the Freedom of Information Act in 2000, the title of Data Protection Commissioner changed to Information Commissioner with effect from 30 January 2001.

The regulator's statutory remit or objectives:

The ICO is currently responsible for the following pieces of legislation:

- Data Protection Act 1998 (DPA);
- Freedom of Information Act 2000 (FOI);
- Environmental Information Regulations 2004 (EIR);
- Privacy and Electronic Communications Regulations 2003 (PECR).

The work of the ICO essentially falls into 2 strands:

- As the **regulator** for Data Protection legislation (DPA and PECR);
- As the **supervisory authority** for FOI and EIR.

The regulator's budget:

The ICO's budget in 2007/08 was £16.9 million. Roughly 65% of its budget funds work on Data Protection and 35% is for work on Freedom of Information.

The ICO receives grant-in-aid funding from the Ministry of Justice for its Freedom of Information work. In the year 2007/08 this amounted to a total of £5.5 million. The ICO's data protection responsibilities are funded entirely by fees paid by data controllers when they notify details of their data processing to the Commissioner. The ICO uses these details to maintain a register of data controllers, which is available for public inspection.

Number of staff (including breakdown of policy and frontline staff):

The Information Commissioner directly employs staff, although job numbers and salary levels are controlled by Government. The ICO currently employs 330 staff in 5 offices situated in Wilmslow, London, Belfast, Cardiff and Edinburgh.

The sectors and number of

The Data Protection Act 1998 (DPA) covers any organisation or individual that processes or holds

businesses
regulated either
directly or indirectly:

personal information either electronically or on paper. This includes for instance banks, credit card companies, sports clubs and Examination Boards. The Act requires all '**data controllers**'² to notify a general description of their data processing activities to the Information Commissioner unless they can rely on one of the exemptions to notification.

As of April 2009 there were 317,165 data controllers registered on the ICO's public register, ranging from central Government Departments and their agencies to small private sector businesses.

² A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

THE HAMPTON VISION

Both the Hampton and Macrory reports are concerned with effective regulation – achieving regulatory outcomes in a way that minimises the burdens imposed on business. Key to this is the notion that regulators should be risk-based and proportionate in their decision-making, transparent and accountable for their actions and should recognise their role in encouraging economic progress.

Any findings relevant to whether the regulator is risk-based:

The ICO deals with a large volume of cases, which reflects the fact that its ambit covers all organisations in the UK that process personal data. This includes, but is not limited to, the 300,000 plus Data Controllers registered with the ICO. Given this large and diverse coverage of regulated entities, it is vital that it has a good understanding of risk in order to operate effectively and without creating undue burden. Indeed, its current level of resources has arguably helped the ICO focus on risk, as it has historically been unable to intervene or inspect as much as it would have liked to.

The review team found that all staff, from the Commissioner downwards, were aware of and able to articulate the importance of risk in matters such as:

- identification and resolution of priority cases;
- choosing whether to audit/inspect businesses;
- deciding whether to take formal enforcement action (e.g. not taking formal action against ‘technical’ breaches);

and, in all those processes, considered the:

- risks of breaches to individuals;
- risks of breaches to society, and
- reputational risks to businesses.

There are also good examples of emphasis on a risk-based approach, for instance:

- the Corporate Plan refers to purposeful risk-based enforcement action;
- the recent Data Protection Strategy endorses a risk-based approach, aimed at minimising the risks for individuals and society when personal data are collected and used – this proportionate approach met with the approval of at least one stakeholder; and
- stakeholders also commented that the ICO took a more pragmatic, less rule-based approach than its peer regulators in Europe and did not

pursue “privacy for privacy’s sake”, for instance regarding sharing of motor insurance database information with the police and DVLA.

However, while the culture of ‘being selective to be effective’ appears to be intuitively well embedded, the review team was not made aware of any evidence of formal or systematic risk analysis, nor documentation of procedures relating to how the ICO takes a risk-based approach. While it is understandable that staff should (and should continue to) draw on their experience, judgment and intuition in reaching decisions relating to risk, the review team considers that it would nevertheless be appropriate and beneficial to record the related principles and procedures – and that this will be all the more important once the ICO increases its level of audit/inspection in response to the greater resources it is about to receive.

The review team also noted that potential extensions to the ICO’s powers of inspection and enforcement, which may or may not be attained to the extent desired by the ICO, will influence the extent to which it can maximise its approach to taking a risk-based approach. Similarly, the recent Data Sharing Review concluded that “data sharing is shrouded in confusion” which has led to a culture that is risk-averse – this confusion can lead to inappropriate secrecy about data with an adverse effect on both business and social policy outcomes. Whilst recognising that work has already been initiated to try and dispel this confusion, and that this is not only a matter for the ICO, the review team suggests that this should be a priority for the new Commissioner.

Any findings relevant to whether the regulator is transparent and accountable:

Stakeholders generally agreed that there was good and timely communication in respect of:

- ICO consultations;
- the development of ICO guidance; and
- clarification of the reasons for ICO decisions (for instance, enforcement notices are published on the website with related press notices).

Indeed, one stakeholder commented that it had “more contact [with the ICO] than with anyone else in the regulatory field”. Another found the recent consultation on a major revision to the ICO’s overarching general guidance “good evidence for the ICO as a regulator drawing on the knowledge and expertise of

practitioners”.

The review team was made aware of a number of instances when consultation had been less than ideal - but these seem to be relatively few. The ICO acknowledged that it had on occasions failed to consult as widely as it should have and has made improvements. This accorded with the team’s findings, although it is nevertheless recommended that the ICO review its stakeholder handling strategy. Doing so should ensure that the ICO is being effective both in being transparent (including covering all major stakeholders and reaching out to small businesses) and in harnessing stakeholders so that it can be more influential, for instance in lobbying for and in respect of the design of any proposals for new regulations.

In respect of accountability, the review team noted:

- support by the ICO during development of sector-produced guidance, which it was subsequently willing to endorse;
- a relatively low proportion of appeals (and few successful ones) against ICO decisions.

In addition, the stance taken by the Commissioner in relation to Data Protection (DP) issues in Europe was much appreciated by stakeholders, especially as it seemed to be having some impact upon the early stages of future development of the legislation. Both the Ministry of Justice (MoJ) and several stakeholders were of the opinion that the ICO was a lead player in the European DP community, and was making real efforts to effect change in the sometimes overly legalistic way in which the Directive had been implemented by some Member States.

Any findings relevant to whether the regulator encourages economic progress:

Overall, the review team did not consider that the ICO was likely to have the potential for as great an impact on economic progress as many other regulators, whose decisions were likely to relate more directly to the business of their stakeholders.

Whilst the ICO does make a small impact on a very large number of businesses, the review team did not identify any significant issues (either Hampton or efficiency related) that would imply that the ICO’s aggregate impact was detrimental to the economy, given that its main activities are driven by its legal obligations.

However, the ICO has some potential sectoral impact, for instance in the context of deciding if certain uses of data constitute direct marketing – an adverse ruling (which of course must be made in the light of the DPA) could restrict the options for and/or efficiency of business-to-consumer communication, with economic consequences. Indeed, at least one stakeholder felt that the ICO could be more proactive in seeking to permit data sharing, when that would be beneficial to business and the UK economy in general, so helping to build a knowledge economy where data could be shared (with appropriate safeguards) to the benefit of both public and private sectors.

The ICO's actions impact upon the economy in other ways and sometimes its decisions to intervene on grounds of data protection or privacy can lead to wider indirect economic benefits, for instance:

- issuing an enforcement notice that stopped the unlawful use of a database used to vet construction workers has potentially opened up part of that sector's labour market;
- enforcement action against cold calling to sell double-glazing, despite consumers having registered with the Telephone Preference Service, should free up human resource for more productive uses.

The review team considers that the ICO follows good practice with its general approach of balancing the nature of any identified breaches and concomitant remedial or enforcement action with the value of what is being protected and/or the potential harm to individuals and/or businesses (for instance, reputational harm should not be disproportionate to the nature of the breach). All staff seemed well aware of the principles of that risk-based approach in the context of audits, inspection and enforcement, noting for example that they would take account of operating/production schedules when visiting and of the actual impact of any penalty on a business. Thus it appears that the actions of the ICO currently impose minimal constraint on economic progress.

However, the imminent new powers for sanctions in the form of financial penalties will increase the extent to which the ICO needs to be aware of its potential economic impact. That is one reason why, as noted by some stakeholders, the ICO should continue to increase the overall level of understanding of business

(especially specific sectors) by its staff, ideally increasing the level of visits to stakeholders to improve its corporate understanding of business systems in practice.

The work the ICO is doing to foster good and efficient relationships with other regulators, including establishing memoranda of understanding with some of them, should help manage different organisational aims and reduce any tensions that might otherwise exist in a way that impacts least intrusively on business. The ICO recognises that there is further work to do in this area but stakeholders recognise that it has begun.

Finally, stakeholders perceive the ICO's approach to decision-making as being more reasonable and pragmatic than that of its European counterparts. The review team notes that this accords more closely with the principles of the internal market relating to data flow and so should correspondingly benefit the economy. This positive impact should be enhanced by the relatively proactive approach taken by the ICO to fulfilling its responsibilities in the context of new technologies compared with most of the rest of the world (including Europe, which is generally at the forefront). The ICO also correctly acknowledges that there is more work to be done on this front.

DESIGN OF REGULATIONS

Hampton principles

All regulations should be written so that they are easily understood, easily implemented, and easily enforced, and all parties should be consulted when they are being drafted.

When new policies are being developed, explicit consideration should be given to how they can be enforced using existing systems and data to minimise the administrative burden imposed.

Key findings on
Design of
Regulations:

- The ICO is unusual among regulators in that it is not responsible to a Minister but reports directly to Parliament. Regulations are drafted and laid by the Ministry of Justice (MoJ). The relationship between ICO and MoJ is working at a basic level but its effectiveness could be improved.
- The ICO should ensure that it consistently provides good quality evidence bases to support its regulatory proposals.
- The ICO is a strong advocate of appropriate regulatory change in Europe.
- Whilst recognising that the ICO needs to maintain its independence, as an organisation it should consider the potential benefits of building closer links with Government. This will enable it to lobby more effectively for change, increased powers and increased resources.
- The ICO has good relationships with its major stakeholders, and consults them on regulatory proposals and statutory codes of practice. However this engagement is not formalised and there is a danger that it is therefore not always comprehensive.

Background
information such as
the regulator's role
in developing
regulations:

Regulations affecting DP and FOI are not made by the ICO, but drafted and made by MoJ (after due discussion with stakeholders, including the ICO). The Data Protection Act 1998 implements a European Directive. Both the ICO and stakeholders accept that UK implementation was over-conscientious in some

respects, but the ICO sees little point in seeking to change the Act now. However, it is actively seeking to influence a move towards reform of the Act by commissioning an independent assessment of the strengths and weaknesses of the Directive (see below).

The previous Commissioner³ saw ICO's priorities as being to continue to 'unpick' the Act, concentrating on three types of role:

- Teacher – to promote good practice, help organisations towards compliance and assist the general public;
- Ombudsman – to adjudicate on complaints brought to the ICO's attention;
- Policeman – to develop the formal powers that the ICO has and use them to enforce and impose sanctions to ensure that legal requirements are followed.

In addition, he considered it important that the ICO positioned the UK at the forefront of recent lobbying in a European context to initiate changes to the Directive.

Any examples of significant good regulatory practice:

The ICO has taken a leading, proactive role in attempts to start a discussion among EU Member States about the continuing fitness for purpose of the Data Protection Directive. This was recognised by several stakeholders, who praised the ICO's leadership in Europe. The ICO takes the view that the Directive is too process-focussed and needs to be recast as a more risk aware, outcome-based legislative tool. The ICO commissioned an independent report (the 'Rand Report') to identify the strengths and weaknesses of the existing Directive, propose ways to improve it and make it better reflect the realities of an IT 'information' age. This report will be presented to a meeting of European DP Commissioners and published in May. The intention is to promote and provoke a discussion with the EU and to instigate steps to re-examine the Directive.

Review findings:

The review team found that the Commissioner and his staff were correct to stress the fundamental importance of the ICO being independent of Government. This is because it regulates the public sector (as well as the

The extent to which the review team

³ At the time of the review, the Information Commissioner was Richard Thomas, who retired from the post in June 2009. Christopher Graham is the current Information Commissioner

believes the regulator is acting in line with the Hampton principles:

private) in its DP work, and in FOI it polices the openness of public bodies. However the team concluded that there was a potential price to pay for this independence, as having no Minister could lead to a diminution of the ICO's influence within Government. Key to whether or not this potential weakness is actualised lies in the effectiveness of the relationship between the ICO and MoJ, the Government Department that drafts legislation.

The review team spoke to MoJ, the Commissioner and his staff about this and concludes that, although a workable relationship exists with MoJ, there is room for improvement, which would yield benefits both in its effectiveness and the efficiency of the relationship itself. The ICO's contact with MoJ is its best chance both to influence regulations and to embed the DP agenda at the heart of Government. MoJ could also, with their cross-government contacts, be a useful ally in the ICO's proactive attempt to shape and drive an EU discussion on the need to change the Directive.

The Commissioner, his staff and MoJ all seemed reasonably content with basic relations – but all commented on relationship issues. For example, MoJ commented that the ICO does not always keep them fully informed of its strategic intentions and policy objectives. This apparent lack of insight and effective communication is manifested most starkly in respect of the ICO's desire to expand its regulatory powers - where it has so far failed to convince MoJ that it has a developed and well thought through plan for why it needs, and how it will use, those increased powers. There is a tension in the relationship between the need for the ICO to retain independence and its need for greater involvement in setting the regulatory agenda - this may be part of the cause of the problems and misunderstandings.

MoJ were asked if the ICO takes enough initiative on regulatory proposals. It was suggested by MoJ that ICO staff are not yet used to or skilled in the policy development process. In addition to the important regulatory powers example discussed in the previous paragraph, a further example of this was the lack, in MoJ's view, of the provision of robust evidence to justify proposals on enhanced powers and the related new fee structure. This could result in fees being set either too high (with an unintended adverse effect on business) or too low (therefore policy objectives would

not be achieved as income would be insufficient to fund them). One way in which the ICO could be up-skilled, and take greater ownership of fee regulatory proposals, is if it was directly responsible for the related consultation and development of the regulations, as is the case with certain other income generating regulators.

However, MoJ were very impressed with how the previous Commissioner had operated within the European Community.

MoJ also commented that the ICO's geographic location contributes to their overall relationship situation. While in the modern world physical location should not prevent effective communication and understanding, the review team considers that this could be enhanced by more face-to-face contact. The need for ICO staff to undertake more field visits with stakeholders is mentioned elsewhere in this report. The review team understands that some effort has been made already but considers that MoJ staff (including legal advisers) would similarly benefit from increased contact and discussions with the ICO's staff at their Wilmslow base, where they would have more opportunity to improve their understanding of the ICO's operations as well as discussing current issues.

The ICO accepted that the relationship with MoJ could be improved, but stressed its disappointment that MoJ have not fully understood nor accepted the need to modernise ICO's powers and processes to a greater extent. The ICO believes that a fundamental flaw with existing regulation is that inspections cannot be undertaken without consent. The current agreements across Government give the ICO this power in respect of government bodies. However, as currently drafted, the proposed regulatory changes will not improve the ICO's access power in respect of private organisations beyond a position where the ICO requires their consent and so cannot undertake an inspection unless they agree. This is seen as a disappointing outcome if it feeds through into the final Act. Although the ICO sees its relationship with MoJ as 'constructive', sometimes it 'can't see where they [MoJ] are coming from.' And, when ICO asks for powers, it sees MoJ as overly driven by legal concerns, conservative and cautious – and without a full understanding of the practical issues.

ICO staff considered that they had given MoJ robust evidence for the powers being requested. They accepted that it was difficult to construct a robust evidential base for the putative effectiveness of new powers, as they have never previously had what they considered a satisfactory inspection regime and so it is difficult to project forward. However, they saw clear political rationale for greater powers, especially following recent high profile data breaches and losses such as the loss of 25 million child benefit records by HM Revenue and Customs (HMRC) and 600,000 service records by the Ministry of Defence.

The review team concludes that this difference of perception regarding the provision of evidence reflected the existence of a misunderstanding, or miscommunication, between the MoJ and the ICO. The team considers that it should be feasible to resolve this situation. If ICO had a more effective voice in Government (whilst retaining its independence) this perception of a difference in requirements for evidence between MoJ and ICO could very well have been resolved at an earlier stage. The review team can take no part or 'side' in this disjunction but, without apportioning any blame, recommends strongly that the ICO develops a strategy of creating and nurturing closer, better and more effective and impactful links with MoJ. This does not mean that all the effort should be on the ICO's part – clearly, MoJ also has a role to play in developing improved links with, and an understanding of, the ICO. We believe that this will not only yield better outcomes but will also result in a relationship that takes up less time in debate and allows more for constructive strategy development.

Turning to implementation and interpretation of the DPA and the Directive, the reviewers were impressed that all stakeholders interviewed were clear that, given that the Directive is interpreted differently across Member States, the ICO demonstrates a good balance between a pragmatic, business-friendly and helpful interpretation and protecting essential individual rights.

There was also good evidence of constructive engagement between the ICO and business stakeholders when drafting and developing statutory codes. A good example of this was the joint work on the Privacy Notices Code, which was informed by consultation, both formal and informal, and a 'critical readers' group of key stakeholders.

ADVICE AND GUIDANCE

Hampton principle

Regulators should provide authoritative, accessible advice easily and cheaply.

Key findings on Advice and Guidance:

- The ICO now consults and involves stakeholders more with the drafting of written advice and guidance. There is much good practice here, but it is not always universal. A formal stakeholder strategy could be developed to facilitate this.
- The good work on the production of the overarching guidance document should be taken forward, and this meta-guidance should clarify the distinction between minimum requirements and best practice.
- The ICO should continue to improve the searchability of its website.
- The ICO should consider ways of improving the staffing and operation of, and also restructuring, its helpline.
- The ICO should take forward improvements suggested by its May 2008 Stakeholder Perception Study and consider developing the benefits of so doing by asking for feedback from users on the helpline.

Background information such as the means by which the regulator provides advice and guidance:

The ICO produces a variety of guidance documents, from statutory codes through to easy-to-read advice on DP for the layman or for SMEs. These are published on its website, with hard copy leaflets also widely and freely available. It holds an annual Data Protection Conference aimed at data protection officers, feedback from which is used to inform and shape the provision of future guidance and advice.

The ICO also operates a telephone helpline service. This helpline deals with both DP and FOI responsibilities.

Any examples of significant good

Stakeholders praised the organisation of the ICO's website into dedicated sections for citizens, data controllers (who should be relatively expert), lawyers,

regulatory practice: etc.

The ICO's prompt and innovative development of Habbo, an online virtual world for young people, was seen as a good response to new phenomena such as the use of social networking sites, as well as other DP issues that affect young people. Discussions with staff yielded a good understanding of the importance of this development and how the ICO's approach engages with the Child Exploitation and Online Protection Centre (CEOP) to protect vulnerable young individuals.

There is good evidence of constructive engagement with stakeholders in the production of some guidance notes, both those produced by the ICO and those produced by some sectoral groups, which the ICO has been willing to review and endorse.

The ICO produces an e-newsletter for stakeholders and data controllers, which now has a circulation list of 6,000 subscribers.

In May 2008, the ICO carried out a Stakeholder Perception Survey on the work of the ICO, to gauge its standing and reputation among key stakeholders.

Review findings:

The extent to which the review team believes the regulator is acting in line with the Hampton principle:

The review team was impressed with the volume of guidance and advice documents published by the ICO, including the efforts made to focus on specific sectors and situations. This reflects the Commissioner's view, as stated to the team, that the ICO is a 'here to help' regulator, whose focus is on trying to guide companies into compliance. Advice and guidance is clearly of key importance if this aspiration is to be fully realised.

The Commissioner, and his staff, also saw the ICO as a 'teaching organisation', reaching out and informing both business and public sector stakeholders and citizens of their responsibilities and rights under the DP and FOI Acts. This is reflected in the amount of guidance that is published, and the priority given to that role by senior management. However, the Commissioner and his staff also accept that at present not enough is being done to proactively engage with stakeholders. This is seen partly as a resource issue, with the ICO wanting and expecting to be able to do more in this area once the new fee structure is in place.

Stakeholders seem clear that guidance published by

the ICO has improved. It is clear and accessible, although sometimes it must also be detailed and technical. One stakeholder commented that guidance sometimes takes too long to produce – for example the guidance on ‘what is data?’.

The ICO has made efforts to distinguish between statutory codes and guidance - but this is still a slightly grey area that could cause confusion to some data controllers; for example, is the guidance the ICO’s interpretation of the DPA, in which case businesses and their legal advisors may or may not agree with it, or does it have legal force? This issue has been addressed relatively recently in the Anderson Review of Guidance and Government’s response to it⁴. Although the ICO has clearly made efforts to engage with stakeholders about the guidance it produces, some still perceive that it needs to engage more with the general business community to establish in what areas guidance is needed, or where current guidance could usefully be improved or developed.

Although there is good evidence of consultation with stakeholders on specific examples of guidance documents, and of this process improving, business stakeholders said that this was not always the case. It was suggested, and the review team endorses this, that a more structured system of consultation on guidance would be better as it can still be a little ‘hit and miss’. The team considers that such a structured consultation system need not be overly prescriptive but would help inform and develop a wider Stakeholder Engagement Strategy, which would be useful to both the ICO and those it regulates.

For instance, stakeholders said that the ICO could involve them in more imaginative ways. Consultation and requests for input are primarily a written process and it would be useful if ICO staff were also more proactive in actually going out to meet stakeholders to discuss their guidance needs and to look at how actual

⁴ **Anderson Review of Guidance**

In the 2008 Enterprise Strategy, the Government asked Sarah Anderson to lead an independent review of the best way to deliver its regulatory guidance. Her report, published on 28 January 2009, concludes that the way Government guidance is currently produced and disseminated leaves SMEs with a great deal of uncertainty, deterring them from using it and creating additional costs. Many are unclear about whether following guidance means they have complied with the law. They do not always know where to get the right help and are put off by the amount of information included in guidance. The report was widely welcomed across the business community and the Government response was published on 5 March 2009 and includes measures to take forward the intention of all the recommendations in the review. The report and response can be found at:

<http://www.berr.gov.uk/whatwedo/bre/reviewing-regulation/The%20Anderson%20Review/page45278.html>

data systems operate in the 'real world.'

There is already some good evidence of the ICO being proactive and reaching out to stakeholders. For example, one trade body praised the ICO both for its well received attendance at events they organise for members and its involvement in looking at and making helpful suggestions on guidance produced by the trade body itself. This stakeholder also said that the ICO takes consultation on guidance seriously and heeds points made during the consultation process, acting upon them where possible.

ICO senior management and staff accept that the provision of guidance is a key area and note that it can also be a difficult one. For example, they stressed that, as the DPA is a principles-based Act, guidance sometimes deliberately had not been too specific - as each 'case' is invariably slightly different and interpretation of the law is sometimes developing, and so it is uncertain what outcome will be reached. This could lead to confusion amongst some target audiences as to whether guidance is interpretative, statutory or a recommendation of good or best practice. The review team recognises this difficulty and commends the ICO for its ongoing project to write and publish an overarching guidance document that will clearly set out what guidance is available, where it is and at whom it is directed. This will be a web-based document with a series of hyperlinks. The team also recommends that the ICO reflects upon how to tackle in that document the issue of the status of guidance.

The ICO has a diverse and varied population of regulated entities and interested bodies and has made good progress in trying to reach out and inform all of them with appropriate guidance. For example, the ICO currently publishes good practice notes in plain English aimed at smaller businesses but issues more technical guidance for larger, more complex businesses and expert users. It is also developing sector-specific signposting to the relevant guidance notes (referred to as 'user journeys', for example on education), which will increase the ease of use of its website and be a useful resource in view of the range of bodies that the ICO regulates.

The ICO runs an Annual Data Protection Conference aimed at data protection officers. Feedback from the conference is used to inform and influence future

policy on provision of advice and guidance, complaint handling and its enforcement strategy.

The Stakeholder Perception Study is another example of the ICO reaching out to those it regulates to gather information that will inform future priorities and actions. There is an action plan to take forward the recommendations arising from this study but not all ICO staff seemed to be aware of this.

The ICO's website, like that of most regulators, is a continual work in progress. The website has a publications directory but ICO management recognises that it is still sometimes unclear which audience is being targeted by which publication. The ICO is actively working to improve this and has an action plan to make the website and the targeting of guidance clearer. Website content is also important as it will impact upon the level of queries put to the ICO's helpline.

Stakeholders recognised that the ICO's website has greatly improved and were largely complimentary, with one citing it as "better than many Government websites". Generally, it was viewed as being of a good overall standard, with efforts being made to develop it. It was seen as containing much useful information that was commendably directed via dedicated sections at a variety of users e.g. business (predominantly relatively expert data controllers), citizens, young people. One good example of this is the ICO's recent, innovation of creating a data protection focussed social networking site for young people (Habbo), including a chat room facility. This is still in its early stages, but has already been publicised with a poster campaign and a TV awareness advertising campaign.

The main criticism of the website was that its navigability and search engine functions needed to be improved, as even regular users could not always find documents – including sometimes ones that they knew existed. ICO staff acknowledged that this is an area to work on and it features in their plans.

The review team shares these views (both positive ones and constructive criticism) and would also recommend that further thought is given to whether the website should be more clearly segmented and so avoid the risks from trying to 'be all things to all people'.

The review team noted with approval that the ICO intends the website to become more of a tool for service delivery than merely a repository of information and is instructing its new website supplier accordingly. The team agrees that this should provide a better and ultimately less burdensome service for stakeholders (both business and citizens). It is recommended as important that the ICO develops appropriate ways of monitoring the impact that this has upon the effectiveness of query resolution. That should also include whether such improvements can be used to help reduce the proportion of helpline queries that could be relatively easily resolved.

The ICO offers a dedicated helpline advice service to its stakeholders, including business and citizens. The helpline staff are relatively junior and are trained before starting but not to develop specialised knowledge – there are not separate helplines for DP and FOI issues, nor is the helpline organised so as to provide a sector-specific service. On a recent visit, representatives of the MoJ sat in on the helpline and were very impressed by the helpful and constructive engagement with both public and business that they witnessed. The ICO also operates a separate helpline for notification enquiries, which is manned by staff from the notification department who have specialist knowledge of the notification requirements.

Stakeholder feedback about the service provided by the helpline has been generally good. One pertinent example in a Hampton context was that the team takes a pragmatic approach to tackling and resolving potential, minor or 'technical' breaches – minimising escalation, which was not the experience stakeholders had with all regulators. However, despite the praise, there was general consensus among those stakeholders (noting that the review team met mainly large ones, who tend to have a good basic understanding of the issues) that the helpline could usefully be improved.

Several stakeholders considered that some of the more in-depth understanding of and knowledge about (more complex) issues relating to specific sectors had declined since the ICO's helpline team had been restructured. This had resulted in a more process-oriented approach, with not very well tailored written responses. One stakeholder noted that these were

less useful, as the responses often included superfluous standard text - this meant overall that business had to spend more time than ideal in identifying what bits of a response were relevant to the resolution of their queries, a burden that should ideally be reduced. Stakeholders also perceived that some advice offered was too legalistic and prescriptive.

Furthermore, it was noted that helpline officers tend towards taking the citizen's side over that of business – partly as they did not always seek business's side of the story before reaching a view. There was also evidence that helpline staff may on occasions give conflicting advice and that the level of understanding that they demonstrated varied (for what is recognised as complex legislation) – though the ICO considered that this might relate to differently phrased, albeit similar, queries. Stakeholders understood that these shortcomings may partly be a resource issue and hoped that would be resolved by the forthcoming increase in the ICO's budget.

The review team followed up all these points and agrees that the ICO should look again at how its helpline works, especially on more complex matters – although it is likely that refinement rather than a major change is necessary. The team considered that the existence of the 'triage' system for identifying priority or complex cases is a good innovation and proving effective but perhaps has not fully bedded in – which is why some inefficiencies have been highlighted by stakeholders (which were all large organisations, with considerable basic knowledge of the DPA and which also had some more complex issues).

The helpline is mostly used by citizens or small business. It may therefore be the case that the advice given does not generally have to be too technical or specialist. The review team noted that helpline staff have had considerable initial training, plus special modules on particular matters or 'hot topics', all of which seemed to be a best practice approach. However, some ICO helpline staff said that they would like to have more training, as both Acts are complex and open to interpretation. Also, especially as some staff are still relatively new, it seems particularly important that less experienced helpline staff are very well trained on when to refer queries and complaints promptly to more specialist or senior staff. Similarly, the supervisory role could be reviewed to check if

enough appropriate support is readily available to more junior helpline staff. Another recommendation would be that the ICO places more emphasis on staff visits to major stakeholders to improve their understanding of specific sectors, including seeing systems in action on-site.

The review team concluded that, although the helpline works comparatively well, the ICO should consider increasing resource and training and, if practicable, restructuring the helpline to reflect the split between the ICO's responsibilities for both DP and FOI.

The review team did not examine in any detail the forms available to communicate with the ICO but noted that an on-line option exists, which is good practice.

DATA REQUESTS

Hampton principle

Businesses should not have to give unnecessary information or give the same piece of information twice.

- Key findings on Data Requests:
- Stakeholders did not consider that the data required to complete the notification process was unduly onerous.
 - However, notwithstanding the legal requirements, stakeholders and the review team queried:
 - the usefulness of all the data supplied, especially the current categories of data use;
 - the validity of the need for an annual renewal.
 - While the ICO makes few requests for data compared to some other regulators, a significant part of its work consists of responding to queries from business and the general public – their efficient handling involves requesting data in the least burdensome way from the person with the query plus sometimes obtaining further information, for instance a business's perspective on a case.
 - Business stakeholders considered that the helpline and website were both useful and worked well but could do with some refinements to improve efficiency and effectiveness – this in turn would impact on the amount of queries and hence data the ICO needs to seek from stakeholders (detailed matters about helpline and website overlap with issues around the provision of guidance and hence are discussed in detail in the above section on Advice and Guidance).

Background information such as the data required by the regulator; the means by which business can return data, etc:

The Data Protection Act 1998 (DPA) covers any organisation or individual that processes or holds personal information either electronically or in structured paper records. Such organisations are known as “data controllers”. Unless the data controller is exempt from the requirement to notify, it must register its name and address and other details on the ICO’s publicly available database.

Notification comprises a general description of the organisation’s data-processing activities, including descriptions of:

- the personal data to be processed;
- the category/ies of data subject to which they relate;
- the purpose/s for which the data are to be processed; and
- any recipient/s to whom the data controller intends or may wish to disclose the data.

The notification procedure can be completed but not, as yet, submitted on-line – nor can payment be made on-line.

If individuals consider that they are being denied access to personal information to which they are entitled, or that their information has not been processed according to the eight principles set out in Schedule 1 of the DPA, they can contact the ICO for help.

Either they can access the website, which is populated with an array of guidance, FAQs and other information, or they can contact the helpline or make a written submission. It is in response to helpline or written submissions that the ICO may need to request further data in order to resolve the query.

The team was informed that there are some 25,000 DP queries and complaints submitted each year in hard copy or electronically, with 70-80% being dealt with by the front-line team and the rest by specialists. 50% are resolved within 30 days, a further 30% within 90 days and some 2,400 cases were unassigned at the time of the review. Less than 1% of cases are appealed (more than that in respect of complex cases), though ICO staff consider that some of these appeals reflect unrealistic stakeholder expectations. Therefore, one challenge for the ICO in reaching its decisions, which

must reflect its assessment of the balance of probabilities of the extent of harm resulting from any identified breach, is to manage stakeholder expectations by making clear the range of potential outcomes - and so reduce the quantity of unsuccessful appeals.

Any examples of significant good regulatory practice:

There is an element of dialogue in the course of the notification procedure, which at first sight might appear cumbersome. However, stakeholders did not appear to find this so and ICO staff were clear that it played an important part in ensuring that data controllers did not just comply superficially with the notification aspect of the DPA but were made fully aware of their wider responsibilities in respect of matters like data security. This approach should foster a culture of compliance and reduce the need for investigation or enforcement action.

The ICO has made some progress with professional associations with respect to encouraging them to make DP notification a condition of the issue of a practising licence (or equivalent) e.g. this has now been agreed for barristers in Northern Ireland. This is a good example of working through others, in appropriate circumstances, and should in turn minimise the burden of ICO contact with relevant, mainly small, businesses to seek such information.

The ICO has relatively recently restructured the way its front-line staff deal with queries and complaints, with a view to reducing what had become an unacceptable backlog. It now makes more use of the website and uses a 'triage' system to focus on the most important or urgent complaints – the previous system had been 'first in, first out'. This has been coupled with several months' initial training of helpline staff, so that they can add value rather than simply provide a functional service.

Review findings:

The extent to which the review team believes the regulator is acting in line with the Hampton principle:

Notification is not only obligatory for organisations (unless they are exempt) but serves a clear regulatory purpose, especially since lack of appearance on the public register is one of the more common sources of public complaints about breaches of the DPA, which all need to be followed up by the ICO. The review team noted that 'hits' on the public register were not recorded and monitored and would recommend that such recording is started.

The renewals procedure, including reminders that are

issued 42 days before the due date, also yields benefits in terms of the ICO keeping data controllers aware of their responsibilities, including the need to keep under review the information they have provided to the ICO. Thus it helps foster compliance in practice, perhaps especially for smaller businesses, and so minimise the potential for harm to those whose data is stored. The review team noted that those who had not renewed were pursued according to the risk the ICO perceived i.e. it focused on larger organisations, those handling sensitive data and smaller outfits affiliated to professional bodies.

In general, stakeholders (the review team met only large business ones) seemed content with the notification and renewals procedures, subject to relatively minor comments reflected below.

The ICO is planning major improvements, to be funded from its increased budget, which include replacement of the current IT system. That in turn will enable notifications, renewals, in-year amendments and payment transactions to be dealt with fully on-line, including on-line submission of forms and increased use of pre-population of data in forms, where feasible. That will be more efficient for both data controllers and ICO staff. These IT enhancements should also increase the potential for communication on-line and for introducing new channels for reminding data controllers that renewal is due - the review team did not explore these in any detail.

The review team discussed the new proposals for tiered fees, which are intended mainly to generate the funds necessary to permit an expansion of the ICO's audit and inspection activity. There appeared to be limited justification for the move to tiered fees in the context of the work necessary in respect of notification and renewal for different-sized organisations. MoJ also seem to have found it difficult to obtain a robust and convincing business case to support the change⁵. However, it was not considered appropriate for the review team to examine what is primarily a resource, not a regulatory, issue further – especially as it seems to be progressing, including with HM Treasury (HMT).

It is, however, recommended that the ICO discuss

⁵ We understand that, since the review the Ministry of Justice has since been satisfied by the ICO's arguments in this respect. The Statutory Instrument implementing this is to be laid shortly.

further with the MoJ how best to structure justifications for any other changes they might wish to make, with a view to maximising the chance of them proving acceptable, with minimal need for discussion. For example, the ICO might in future consider that an increase in fees or a change to the three-tier structure is desirable. To justify and progress any such changes, it is essential that MoJ/ICO are able to provide robust impact assessments to accompany the formal consultations that are required on new legislative proposals.

The organisational changes to dealing with enquiries and complaints seem to have proved largely successful. However, staff resources have not been stable enough for a conclusion to be reached about resolution of the backlog (which has been exacerbated by a 'spike' in new cases due to the impact of the issue of 'unfair banking charges' – even though that is not strictly a DP issue). However, it seems a little disappointing that 2,400 cases are yet to be assigned for resolution, although the review team understands that it is only recently that the front-line team has become fully resourced, with half of its staff being relatively new. The ICO is considering how best to reduce the backlog, especially as most of the complaints about the ICO (as opposed to about the DPA) relate to slow turnaround of cases – the review team endorses that this should be accorded a high priority.

INSPECTIONS

Hampton principle

No inspection should take place without a reason.

Key findings on
Inspections:

- Harm to the individual is understood as the key risk that the ICO seeks to prevent through its Data Protection regulatory activity.
- Risk assessment is made on intuition rather than following a systematic methodology.
- The ability to conduct inspections (audits) is limited and therefore they are more likely to occur in compliant businesses that volunteer for an audit to complement their own internal assurance processes.
- New powers are needed, and are being sought, to enhance the ICO's regulatory effectiveness.

Any relevant background information such as the number of inspections and the number of businesses inspected; the regulator's risk model etc

The ICO conducts criminal investigations and non-criminal investigations, including compliance (good practice) audits.

It has sought and secured a high public profile for its criminal investigations in relation to section 55 Data Protection Act 1998 offences. Notable examples of investigations have been in relation to discovery of both a secret construction database and "blagging" activities by private investigators.

To enable effective criminal investigation it has the power to seek a warrant for entry into premises to secure evidence. Cases are referred to the investigation team by front line enquiry staff, who may identify situations that they think indicate the commission of a criminal offence. The investigation team, currently four strong but due to increase to five, reviews these referrals and determines whether they are taken on or are more suitable for another action (for example, an audit) or none at all (for example, a financial adviser who has left and uses his previous contacts list - this would be suitable for resolution through discussion with the previous employer). There were 230 referrals to the investigation team in the last

year, not all of which necessitated a criminal investigation. ICO's current investigators come mainly from a police background. Opportunities for joint investigation on cases of mutual interest are sought, and have been carried out with HMRC and the Department for Work and Pensions (DWP).

Audits can currently only occur when an organisation consents. It is a completely voluntary agreement. 50 audits have been carried out in the past five years. There are currently nine audit staff, half of whom are relatively new. Auditors are trained internally. However, external training and assistance in the evolution of the audit methodology was obtained from a private specialist audit company.

The ICO aims to audit for compliance in the following situations:

- An organisation volunteers;
- An organisation is identified in a sector where a number of issues have been identified and consents;
- It is part of an agreed good practice audit of a Government Department (e.g. DWP; DVLA);
- The audit is agreed as an outcome of enforcement action;
- It is an audit with EU partner data protection regulatory bodies from the Article 29 group (there has been one so far).

Feedback is provided at the time of an audit. This is followed up with a written report, consisting of two parts: an adequacy report; and a longer assessment of compliance.

The ICO is seeking new inspection powers, to enable "non-consensual" right of entry to conduct compliance inspections. This would enable the ICO to tackle areas of risk of non-compliance that are not appropriate to be handled through criminal investigation.

Any examples of significant good regulatory practice:

Effective investigation, where there was a risk of harm to individual data subjects, was identified in cases discussed elsewhere in this report, which the ICO has investigated (e.g. construction; "blagging").

However, the review team concluded that ICO is not as

effective, as it could and wants to be, in the area of audit inspections. This is because it is hampered in being risk/intelligence-led by the current constraints on its inspection powers, particularly as any audit inspection has to be with consent of the organisation that is to be inspected. Currently, ICO inspectors are unable to conduct surprise audits with the power of entry, backed also by an offence of obstruction for non-cooperation/access.

Review findings:
The extent to which the review team believes the regulator is acting in line with the Hampton principle:

Richard Thomas, the previous Information Commissioner, had stated that the ICO needs to be “selective to be effective”. The current process is predicated mainly on an intuitive understanding of risk that draws on the career experience of ICO staff. There is at present no risk assessment methodology or strategy for the introduction of any such more formal approach. This, itself, is therefore a risk to compliance with the Hampton principle. However, this concern has to be balanced against the current situation, which does not result in a significant number of audit inspections - and they cannot really be seen as a burden, as they only occur through agreement and consent.

High profile losses of data have raised the public's awareness of data protection issues and it is recognised that this has created a demand for greater inspection powers. Such powers are currently being considered in Part 8 of the Coroners and Justice Bill. If secured, they may result in an increase in inspections. Any such increase will need to be justified in the light of robust evidence of sectoral or individual business risk. This will require more emphasis on selectivity to ensure that the ICO focuses on the areas of greatest risk.

The introduction of an “intelligence hub” to provide an analytical centre to prioritise, allocate, and determine the approach to take (i.e. criminal investigation or audit) is recommended. Such a hub should consider adoption of the appropriate elements of the National Intelligence Model, complemented by a risk scoring mechanism based upon the areas identified in the Data Protection Strategy. We also recommend that the ICO looks at how other regulatory bodies are developing a risk-based inspection regime, and considers how this is used to support their powers of entry (and how they are legally constructed) with a view to learning from appropriate best practice.

The review team commented earlier on the current relationship with the Ministry of Justice (MoJ) and its requirements for business case justifications for legislative changes. Critically, this may impact upon the nature of the powers currently being sought, resulting in powers that do not effectively assist the ICO in achieving the regulatory outcome it believes necessary. The MoJ view was that the ICO were seeking new powers to obtain a warrant for entry based on risk analysis, but that no specific evidence had been provided regarding this particular point and it could not see a justifiable case. Some other stakeholders seemed to infer that the ICO was seeking a power to conduct random inspections - if this is accurate, such new powers would not appear to be in accordance with the Hampton principle. However, the review team considers that there is a lack of mutual clarity over what the ICO wants, which must be resolved if the ICO is in future to justify and secure new inspection powers that comply with the principle. The team also notes that peer data protection regulators in Europe are able to enter premises without business' consent.

It is clear from interviews with ICO staff that they do not want to merely use evidence of specific potential risk to justify a warrant for entry to premises; they cannot because such an approach would be inconsistent with the rigour required by a court to approve the issue of a warrant to support a criminal investigation. Nor does the ICO want a power of random inspection – for instance, it would select for inspection only businesses about which it had received complaints and when it considered that the nature of the likely breach had the capacity to harm individuals.

Interviews with senior staff indicate that what the ICO seeks is a power to enter premises to inspect, when it has relevant indications of risk and non-compliance and to do so, where appropriate without notice. Formally requiring the ICO to provide advance notice in all cases would be counter-productive, particularly where a risk/intelligence-led methodology indicated there was a risk of destruction or suppression of documents or databases to be inspected. Therefore a power of entry that the ICO can use selectively and proportionately, without a legal constraint on the need for advance notification, would enhance the effectiveness of the inspection regime going forward.

The ICO also believes that it would have a considerable deterrent effect, as discovery by this means of breaches that required sanctions (especially if those included new administrative penalties) would be given due publicity.

At present, the ICO has not succeeded in having this desired power of entry reflected in the Coroners and Justice Bill. It is recommended that the ICO urgently discuss their future operational requirements to ensure that the MoJ understands how they wish to use new powers, in what circumstances, and how such circumstances would comply with current court operations and be guided by risk assessment in accordance with the Hampton principles.

Finally, the review team looked at a sample audit report and suggests that audit recommendations are in future stratified to indicate their relative level of importance, especially if there are many of them. That will be more transparent and also make it easier for the business to take corrective action in line with better regulation principles, homing in on the biggest risks first.

SANCTIONS

Hampton & Macrory principles

The few businesses that persistently break regulations should be identified quickly and face proportionate and meaningful sanctions.

Regulators should be transparent in the way in which they apply and determine administrative penalties.

Regulators should avoid perverse incentives that might influence the choice of sanctioning response.

Regulators should follow up enforcement actions where appropriate.

Key findings on Sanctions:

- The ICO publishes its principles on regulatory action and sanctions but they need to be given higher prominence on the website.
- The ICO aims to provide a proportionate sanctioning regime and will be implementing new sanctions, as passed in the Criminal Justice and Immigration Act 2008 (section 144).
- The only current alternative to prosecution is a caution but that may have limited effect and deterrent power, as it is not citeable on criminal records.
- Changes from the 2008 Act and those proposed in the Coroners and Justice Bill suggest that there has been limited consideration of whether Macrory penalties would further enhance ICO sanctioning options.

Background information such as a summary of sanctions available to the regulator and any data on sanctions imposed by the regulator:

There are several criminal offences that may lead to prosecution. These include offences of obtaining and misusing data and the offence of failing to notify the ICO that an organisation is processing relevant personal data. Most prosecutions currently are for the offence of failing to notify. This appears to be a simple offence and in itself is at the lower end of the scale of seriousness of offences – though it could be symptomatic of more serious offences relating to unintentional, or deliberate, misuse of data.

Any examples of significant good regulatory practice:

The ICO considers “naming and shaming” when it has sanctioned an organisation. However, it is quite correctly also aware that publicity could adversely affect data subjects. When it considers that greater harm could arise through publicising its regulatory outcomes, it will avoid doing so. Such a process avoids unintended consequences, whilst proactively seeking to create prevention and deterrence publicity as far as is possible.

Review findings:
The extent to which the review team believes the regulator is acting in line with the Hampton principles and Macrory characteristics:

The ICO publishes significant guidance on its website. This includes its Regulatory Action Strategy. The document provides a good summary of its powers and current sanctioning options, and reflects the five principles of good regulation from the Enforcement Concordat. However, the publicly available document was produced in November 2005. Furthermore, it is not easy to identify, appearing within a considerable list of publications⁶. The new sanctions, which may be implemented in October 2009, will require a review of this document. It is recommended that such a review takes account of the guidance on the Regulatory Enforcement and Sanctions Act 2008 (RES Act) on producing penalty guidance and an enforcement policy.

It is further recommended that greater prominence on the website is given to the document to enable the public and data controllers to more easily access advice about the consequences of committing breaches of legal requirements.

There is no evidence that the current sanctioning regime is informed by risk assessment. Prosecutions, however, are considered against the Code for Crown Prosecutors, which includes a public interest test. Nonetheless, when the ICO implements new sanctions and revises its guidance, an opportunity exists to consider how to incorporate risk assessment into its decision-making process.

The review team noted that the ICO monitors the effectiveness of the enforcement notices it issues, for instance by keeping an eye on the level of complaints

⁶ The document was identified on a search for “regulatory action”, which may not be obvious to the public, or through the publications list to:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_strategy.pdf

– taking follow up action if it seems necessary. This is a sensible part of a risk-based strategy.

Finally, it is recognised that the ICO is entering a period of change, with a number of legislative changes ahead. Despite these, it is recommended that the ICO considers further, and relatively soon, the opportunities presented by the expanded toolkit of sanctions available under the RES Act (Macrory powers) and whether they could be used to address offences (such as a section 17 failure to notify) by alternative and proportionate means. This would inform the ICO's strategic approach to sanctions and, if adopted, enable a more proportionate approach to dealing with cases where the harm created by the offence is less direct and immediate. It would thus assist in directing resources to more serious, time-consuming and costly offences.

FOCUS ON OUTCOMES

Hampton principle

Regulators should measure outcomes and not just outputs.

Key findings on
Focus on Outcomes:

- The ICO has clear processing output clearance targets.
- Desired organisational aims are understood by staff, consistent with the Data Protection Strategy, and this has been evidenced in the staff survey.
- There has been high profile publicity for a number of successful ICO investigations, which raise awareness of data protection, and which represent effective outcomes consistent with the ICO's mission.
- Outcome targets, or a reflective narrative on successes, are not fully developed and embedded into corporate/business plan targets and annual reports.

Background
information such as
the regulator's key
objectives:

The ICO's key objectives are set out in the ICO Summary Business plan for 2008/09. However these objectives are output-related, and do not detail planned activity to achieve regulatory outcomes that improve data protection compliance and behavioural change.

Such objectives are more effectively articulated in the Data Protection Strategy.

Any examples of
significant good
regulatory practice:

Securing effective publicity on high profile investigations enables the ICO to demonstrate an ability to achieve outcomes consistent with its strategy, notably where harm can most easily be demonstrated.

In relation to the high profile data losses by HMRC, the ICO contributed its views and awaited the report commissioned by HMRC. This avoided creating extra burdens but enabled the ICO to make use of the report to determine what undertakings it would require to ensure HMRC's future compliance. The ICO therefore focused on the outcome it required rather than

engaging in a complicated audit of HMRC (although it may, quite properly, do this at some future point as part of its good practice audits of Government Departments).

The work on the Personal Information Promise – securing CEO sign up to the promise to be accountable for data protection - is a good example of engaging with stakeholders to create a framework of compliance, with an outcome of raised awareness and accountability.

Following successful action taken against private investigators who had illegally ‘blagged’ information from BT about customers, the ICO further demonstrated its impact by producing two reports: “What price privacy?” and “What price privacy now?”. The value of these documents is that they demonstrate how evidence of successful investigations can build an effective case for new powers and sanctions, making best use of outcomes that are coherent with the ICO vision. In turn, this created the desired outcome of securing new sanctions.

The extent to which the review team believes the regulator is acting in line with the Hampton principle:

In line with other regulators (and many other organisations), the ICO has output measures and performance indicators that assess operational performance. This is not wrong but the review team does not consider that this goes far enough - there is still an absence of outcome measures at the ICO, which is of particular interest as good publicity of its impact can in itself help further the ICO’s objectives. This should not be seen as a serious criticism of the ICO but an area that merits reflection and development, especially with the organisation’s resources about to increase.

Insufficient outcome measures have already been noted in a number of Hampton Reviews. However, the review team recognises also that effective measurement of outcomes is difficult – especially for an organisation like the ICO that relies upon third parties to report transgression of the law (and so has a considerable proportion of demand-led work).

In considering how to measure outcomes against its vision the ICO needs to consider that outcome targets need not be numeric – they can perfectly validly relate to interventions and actions whose achievements can be demonstrated narratively, for example in its annual report, which reflects on successes within an

operational year.

Whilst the review team's discussions with staff in focus groups provided recognition that there was an understanding of the ICO's core objectives and its harm-based model for prioritising interventions and actions, there was little evidence of understanding what outcome targets should be. Nor was the thinking well formulated among senior management, with whom the team had productive and constructive discussions on the topic.

The ICO has had some high profile successes (many of which are referred to earlier in this report – both in generating awareness and encouraging compliance and in identifying and enforcing against major transgressions). And it has made effective use of them in press releases and reports. However, the review team considers that there is a gap where the ICO has not yet recognised how to incorporate such successes into an ongoing narrative of its outcome achievements. And, as well as making things clearer for external stakeholders, increased clarity in this area should also prove beneficial for ICO staff morale.

There is therefore room for development in respect of the ICO's use of its successes, including embedding the awareness of those successes as a demonstrable focus on outcomes by its staff.

Nonetheless, the review team was encouraged that the ICO monitors each year the level of awareness both of organisations about their obligations and of individuals about their rights. The aim of so doing is to assist the ICO in creating a climate of compliance for business and other organisations and assessing its own effectiveness in knowledge building of Data Protection issues among the general public.

**Appendix 1:
Review team
membership**

Martin Bagwell is a policy civil servant at the Medicines & Healthcare products Regulatory Agency (MHRA), an Executive Agency of the Department of Health. His responsibilities at the MHRA include Better Regulation, in particular taking forward work on embedding the Hampton principles within the MHRA and chairing a working group that is looking at the applicability of the Macrory toolkit of sanctions to the MHRA's enforcement and sanctions regime. He also has responsibilities for open government policy within the MHRA.

Darryl Dixon is Director of Strategy at the Gangmasters Licensing Authority (GLA), responsible for developing new powers, regulatory & enforcement approaches and international exchange agreements. Previous GLA operational roles covered: compliance, enforcement, intelligence and licensing. He has also worked in licensing at the Security Industry Authority and in the professional standards unit of the Counter Fraud Investigation Branch of DWP. He is an Accredited Counter Fraud Manager; holds an MSc in Security Management and is a Fellow of the Security Institute.

Peter Gartenberg is a policy civil servant at the Department for Culture, Media and Sport, currently Head of Financial Policy. His previous post there included sponsorship of the Gambling Commission and dealing with Better Regulation gambling matters. At the time of the review he was on secondment to the Better Regulation Executive. He is a Chartered Accountant, with experience prior to joining the Civil Service mainly in auditing and industry.

Better Regulation Executive
Department for Business, Innovation and Skills
3rd Floor
1 Victoria Street
London SW1H 0ET

Website: www.berr.gov.uk/bre

URN: 09/1347

© Crown copyright 2009

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to material not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when being reproduced as part of another publication or service.