

The Information Commissioner's Inspection Powers and Funding Arrangements under the Data Protection Act 1998

Response of the Information Commissioner to the Ministry of Justice's Consultation Paper of 16 July 2008

SUMMARY

- 1 The Information Commissioner (IC) welcomes the Consultation Paper. He also welcomes the Government's intention to give effect to the recommendations in the Data Sharing Review relating to his powers of inspection and the funding arrangements for his office. These recommendations are consistent with the proposals he has put forward previously, most notably in the paper on Data Protection Powers and Penalties that he submitted to the MoJ in December 2007.
- 2 However the IC has reservations about the precise mechanisms proposed by the MoJ for implementation. These are most significant in relation to inspection powers where the IC fears that the proposed consent based model, with the fall back of a search warrant, will be hard for data controllers to understand and cumbersome to operate in practice. He commends the approach taken in the Republic of Ireland that is referred to in the Data Sharing Review where the Data Protection Commissioner has a simple power of inspection that appears to operate well in practice.
- 3 The IC welcomes the proposal to increase his information notice powers under Section 43 of the Data Protection Act but reminds the Government of his need to be able to serve a notice on any person rather than only on the data controller. He also finds much that is attractive in the Government's proposals in relation to his powers of entry to premises but wonders why the existing Section 54A of the Data Protection Act relating to the inspection of overseas information systems has not been used as the basis for further development.
- 4 So far as funding is concerned the IC favours the introduction of a tiered fee structure as proposed in the Consultation Paper, but is concerned that basing the tiers on EU definitions of small, medium and large enterprises might not be represent best regulatory practice. He would prefer the tiers to be based on an estimate of the number of individuals an organisation processes personal data about. The IC is also concerned at the risks involved in exempting significant numbers of data controllers who are currently required to pay a notification fee from having to do so in the future.
- 5 The IC reminds the Government of the need to resolve the position of small CCTV users so far as notification is concerned. He also agrees that there should

be a penalty for data controllers who knowingly or recklessly provide incorrect information as part of a notification fee assessment.

INSPECTIONS – A BETTER WAY

- 6 The case for an inspection power for the IC has been made many times. It is taken up in the recommendations of the Data Sharing Review (Recommendation 12), which itself involved a wide ranging consultation and it is reflected in the Consultation Paper. It is though worth stressing that an inspection is not a punitive measure. It is part of the process of promoting good practice and providing advice on standards that is, and will remain, key to the IC's regulatory role. However for this process to be truly effective it is important that organisations can not "opt-out" of the possibility of an inspection and that if serious wrong doing is found the IC has tools at his disposal that he can use to ensure that compliance is achieved. An inspection is, as the MoJ says of the proposed good practice assessment, not a power but a tool. The tool will not though be truly effective unless it is supported by a power to use it.
- 7 The IC is attracted (with some modification) to the approach taken in the Republic of Ireland. This is commended by the Data Sharing Review (Paras 8.62-8.64) and is elaborated in the attached annex which helpfully has been provided by the Irish Data Protection Commissioner. The need for what are termed "aggressive inspections" is already catered for in the UK by the IC's power to obtain a search warrant under Schedule 9 of the Data Protection Act. However the legal provisions and practice relating to "routine audits" provide a simple, common sense model that, in the Republic of Ireland, works well and would bridge the gap in his powers that in the UK the IC is keen to address. The IC is attracted to the Irish model, as was the Data Sharing Review (Para 8.63), in particular because of the flexibility it provides. This flexibility can be used to deliver a risk based approach, ensuring that any regulatory activity is appropriate to the circumstances whether it takes the form of a spot check of a particular site or activity, a more wide-ranging inspection or a full audit.
- 8 The Irish model has been in place for some time, appears to work well, is accepted by the business community and is based on the same framework of European Community and human rights law that applies to the UK. Furthermore the IC does not believe that any doubts have been expressed as to whether the Irish Model meets the requirements of Article 28 of the EU Data Protection Directive (95/46/EC). It is therefore difficult to understand why the MoJ appears to favour a much more complex, untested approach that almost certainly carries greater risk of failure than an approach modelled on Irish law and practice. The Irish experience does not bear out the fears expressed by the MoJ in its evidence base that giving the IC a general power of inspection would be disproportionate and thereby alienate data controllers. There is no evidence to support this whereas the evidence from the Republic of Ireland is that it would not. Furthermore, the evidence from the Data Sharing Review is that data controllers support stronger powers for the ICO, ("We received an overwhelming body of evidence that the IC's existing regulatory powers are too weak for him to carry out his job as effectively as he should" - Para 7.6).

- 9 The IC does recognise that there are genuine concerns about giving his staff unfettered access to business premises to carry out random inspections. This is not what he is seeking. The practical approach that is adopted in Ireland is consistent with the IC's ambitions. He would not therefore have any difficulty with suitable judicial oversight and statutory or other obligations designed to ensure that this is how he acts in practice. In particular he would be happy to have constraints placed on him to ensure that:
- the selection of organisations for inspection is based on an assessment of data protection risk;
 - organisations are not subject to random inspections albeit that there might be an element of sampling amongst organisations that fall into high risk categories;
 - organisations are given reasonable notice of a planned inspection with sufficient time to prepare;
 - organisations are given an explanation of why they have been selected for inspection;
 - organisations have a right of appeal to the Information Tribunal (or to a court) if they receive notice of a planned inspection and consider that they have been selected unreasonably or have other grounds to object;
 - in recognition of Human Rights Act considerations any power to enter an organisation's premises does not extend to domestic premises;

These constraints could be spelt out in the legislation or, with other good practice obligations, could be embodied in a code of practice. Such a code could either have statutory authority or be laid before Parliament. The IC would be obliged to observe the provisions of the code in his inspection activities.

PROPOSAL 1: PROMOTING GOOD PRACTICE

- 10 The IC understands the intention behind the Government's proposal to allow data controllers to provide their consent for a good practice assessment when they register. To the extent that it might enable a much wider range of inspections to be carried out than is the case currently it would be welcome. However the IC considers that whilst the proposal is inventive it is largely impractical. In line with good regulatory practice the ICO has done much to streamline the notification process for data controllers. It wishes to continue this process of simplification in so far as the legislative framework allows.
- 11 The Data Sharing Review expressed a very clear belief "that it is important that inspections should not have to depend on the consent of the data controller" (Para 7.9). Asking data controllers whether they consent to a good practice assessment (GPA) when they notify will add complexity to the notification process, make it more time consuming, and will run counter to the Hampton requirement for fewer, better forms. The register currently includes in excess of

300,000 data controllers. They will all have to be asked for consent as will any new data controllers seeking to notify for the first time. It is not clear from the consultation paper whether this will be on an opt in or an opt out basis. Data controllers will have to weigh the pros and cons of giving consent. In the early days at least, there will be understandable uncertainty as to exactly what an assessment will entail. It will though be genuinely difficult to advise even in general terms on the organisational effort involved given that, in practice, the nature and extent of each inspection will depend very largely on particular circumstances such as the volumes and types of processing. It should be possible to give some guidance on the process an assessment might follow but the suggestion in the consultation paper that there is a some kind of “standard assessment” the scope of which could be explained to data controllers is mistaken.

- 12 The ICO’s experience suggests that significant numbers of data controllers will seek advice. Even if only 5% contact the ICO in the first year this will mean 15,000 additional contacts or roughly 60 every working day. The problem is compounded by the fact that for the vast majority of data controllers the question of whether to give consent, which necessarily involves an element of judgement, is a purely academic one. All data controllers will be required to put their mind to the question when in fact significantly less than one in a thousand will be selected for an inspection in any one year. The IC disagrees therefore with the MoJ’s suggestion that the burden will be minimal or that asking all data controllers for consent is consistent with good regulatory practice. Indeed it is arguable that simply asking this question of so many will by itself impose a greater burden, at least in the short term, on the business community as a whole than would the inspections themselves were the IC to be given a direct power that led to the conduct of somewhere in the order of 120 inspections per year.
- 13 The IC is concerned at the lack of evidence behind the MoJ’s suggestion that giving data controllers an exemption from a civil monetary penalty will provide a significant incentive for data controllers to volunteer consent. The IC understands the desirability of providing an exemption for other reasons, but, in reality, less than 0.1% of data controllers will face a GPA in any one year and the likelihood of finding a breach that would justify a penalty will be slim. This means any incentive effect is likely to be minimal. In fact we see it as much more likely, based on our current experience of auditing, that data controllers will take a cautious approach. Particularly if they are in the private sector and they receive legal advice, they are unlikely to expose themselves to the risk, whether real or perceived, that giving consent to a GPA might bring.
- 14 The IC is also concerned at the risks inherent in developing different approaches to inspection for the public and private sectors. He has already been assured that his staff will be able to undertake “spot checks” of Government departments without specific reasons, consent or a court order, albeit that the details of how this will work in practice are still under discussion. He can do little more than reiterate the observations of the Data Sharing Review that, “The regime of spot checks being introduced for central government departments needs statutory authority if it is to be viable and sustainable, and we note that the commitment to extend the regime to the rest of the public sector has yet to be fulfilled.

Distinguishing between public, private and voluntary sectors makes little sense, especially as more information is shared across sectors whose boundary lines are forever shifting” (Para 7.9).

PROPOSAL 2: ENFORCING COMPLIANCE

- 15 The IC welcomes the proposal to increase his powers to obtain information under section 43 of the Data Protection Act. This is consistent with the findings of the Data Sharing Review (“Key to promoting and enforcing standards of good practice is the regulator’s ability to obtain information from a regulated body” Para 7.8) In addition the IC wants to remind the Government that he has previously sought an extension of his information notice powers to enable him to serve a notice on “any person” rather than just “the data controller”. This is because there 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.
- 16 There is much that is attractive to the IC in the Government’s proposals in relation to the power of entry to premises. The IC is committed to a risk based approach to all his regulatory functions so would apply the principles set out in paragraphs 58 to 63 whatever the means by which he is able to gain access to a data controller’s premises. He wants to stress that he is not seeking a power to conduct entirely random audits. However, as outlined above, he would prefer a simple power to enter premises to conduct an inspection, with appropriate notice requirements and accountability mechanisms to ensure the power is used responsibly, to the more burdensome and confrontational approach of applying to a judge for a warrant. As the Data Sharing Review recognises, “To check an organisation’s compliance with data protection requirements may take some time, usually on-site, examining how policies, procedures and technologies are operating in practice and checking management and staff behaviours” (Para 8.63). This is not a process that sits comfortably with the use of search warrant powers.
- 17 The IC’s experience with warrants suggests that a judge will expect the IC not only to specify the premises he wishes to enter but also to specify what he is looking for. This degree of formality is appropriate when seeking evidence of criminal offences but unhelpfully restrictive when the aim is to encourage compliance. As the Data Sharing Review confirms, “A search warrant can only be obtained in limited circumstances, is more suited to criminal misconduct and is not suitable in cases requiring a fuller inspection than can be carried out on a single visit or by seizing equipment” (Para 8.64).
- 18 The IC notes the reference in paragraph 44 of the consultation paper to the IC’s power under section 54A of the Data Protection Act to inspect overseas

information systems. This is a power that the IC has used to conduct constructive inspections in the past. He wonders whether the MoJ have asked those subject to these inspections about their experience and why the MoJ have not used this power as a basis for further development. It would appear to provide, with some modification, the basis for an inspection regime along with lines the IC is advocating above. It does not though feature in the options under consideration and the reasons why it has been discarded are unclear. It is also unclear whether the MoJ intend that the powers under section 54A will remain. If they do the risks associated with developing different approaches to inspection for different sectors referred to in para 14 above, are enhanced. If they do not the UK's compliance with the international legal instruments establishing the relevant information systems may be called into question.

PROPOSAL 3: FUNDING

- 19 The IC agrees with the recommendation of the Data Sharing Review that his Office should receive a significantly higher level of funding (Recommendation 13). This is necessary not just to carry out his existing statutory duties, but also to fund the additional data protection responsibilities covered by the consultation paper. He also agrees with the proposal that the additional funding should be introduced by means of a tiered notification fee structure. He believes that the introduction of a tiered structure is the right way forward so that those who place the greatest demands on his regulatory resources (that is those who pose the greatest data protection risk) contribute the most towards them.
- 20 In the light of this the IC has doubts whether it is appropriate for tiers to be based on EU definitions of small, medium and large enterprises. Although it is true that as a generality larger enterprises place more demands on his office than smaller ones it is by no means true that there is a direct correlation between data protection risk and size of business. A large manufacturing business where personal data processing consists mainly of HR records, may pose a low data protection risk when compared to a small online retailer of medical products with a large customer database containing sensitive personal data. As the Government recognises in its own data handling procedures data protection risk is directly related to the extent and nature of personal data processed, rather than the size of enterprise. The IC has already conducted some market research amongst a sample of registered data controllers. This indicates that a model in which the tiers are based on an estimate of how many individuals an organisation processes personal data about is workable and is considered preferable to a model based on either turnover or number of employees. The IC is a little surprised that the evidence provided by this market research (http://www.ico.gov.uk/about_us/research/data_protection.aspx) is not cited in the evidence base attached to the consultation paper. An approach based on extent of personal data processed is the one the IC would prefer.
- 21 The IC is seriously concerned at the risk to his funding posed by the suggestion that some smaller organisations that are currently required to notify might be completely exempt from payment. He reminds the Government that there are already significant exemptions from the requirement to notify, and hence to pay the associated fee. Very many small organisations already take advantage of

this. The IC knows that the current notification regime produces an income of around £10.5 million. Requiring a proportion of those notified to pay a higher fee can only increase his income. Although some modelling has already been undertaken, and further work is required, the impact of introducing a higher fee tier can at best only be estimated. If the estimate turns out to be wrong the IC may not get the increase in funding he was expecting (or he may get more) but his existing funding is not at risk.

- 22 The modelling that the ICO has undertaken so far has been based on the assumption that all those on the existing register would continue to pay a fee. If significant numbers who currently pay cease to do so in the future the risk attached to estimating the impact of cut off points is much greater. In the first of the variations offered in Annex One to the consultation paper 35% of data controllers currently on the register would pay £80 and 5% would pay £500. This would produce an increase in fee income to roughly £16 million. However if the cut off points which are designed to deliver these proportions in fact only deliver 25% at £80 and 3% at £500 the ICO's income will remain at the present level of £10.5 million. It is even possible that there could be a net reduction. Given the uncertainty attached to modelling cut off criteria against the current register, particularly where smaller data controllers are concerned such variations are well within the bounds of possibility.
- 23 The IC is also concerned that both the examples used in the consultation paper show as many as 40% of data controllers paying more than double the current fee of £35. This could be highly controversial. He appreciates that these are only examples but on the risk related approach he favours he would find it hard to justify a significantly increased fee for more than the top 10% or so of data controllers. He also doubts whether the "better regulation" message or the silent majority who will benefit will do much to temper the likely outcry should as many as 120,000 data controllers be asked to pay more than double their present fee.
- 24 The IC would therefore prefer an approach that maintained the existing fee for almost all data controllers. Using an approach based on the ICO's own research (referred to above) would allow the fee to remain unchanged for 85-90% of data controllers with a fee of £250 for the 10-15% of data controllers who process information on more than 100,000 individuals. This would result in the regulatory burden remaining unchanged for the vast majority, but increasing for those who pose the greatest risk and make the greatest call on the ICO's resources.
- 25 If the fee is based on the EU Definitions of small medium and large enterprises the IC would prefer the fee to remain at £35 for all small and medium enterprises who are currently required to notify, with an additional fee only being charged on those businesses falling into the EU definition of a large enterprise. This would approximate roughly to the suggested 5% of data controllers paying the highest fee as contained in Annexe A of the consultation paper. The IC would also point out that these EU definitions would need to be considerably refined to apply in some areas, particularly the public sector, partnerships and charities (that are not otherwise exempt) because of accounting differences. This is likely to add complexity to the process.

- 26 The IC wishes to remind the Government about the position of small CCTV users. In the light of a number of developments the ICO has revised its guidance to the extent that, in its view, small users of CCTV are now caught by the requirements of the Data Protection Act. This position is reflected in the ICO's recently updated CCTV Code of Practice. From a public policy point of view the IC considers it right that even small CCTV should be subject to the good practice requirements by the Data Protection Act and ultimately to his enforcement powers. He has though been concerned that requiring such users to notify and pay the associated fee would be seen as an unwelcome and disproportionate imposition on small businesses and would in practice, add little to the protection of the public. It appears to the IC that there is now an opportunity to introduce an exemption from the requirement to register for small CCTV users who would otherwise be able to rely on the existing exemptions aimed at small businesses. Alternatively, if notification is considered appropriate in the light of the Government's national CCTV strategy, there is an opportunity to simplify the requirements and/or remove the fee.
- 27 More generally the IC is willing to look at notification requirements to examine whether, when a tiered fee is introduced, these can be simplified further. Whilst the IC has to work within the confines of the relevant legislative framework and bear in mind that the primary purpose of the register is transparency he will consider whether it is possible to reduce the burden of notification still further for some if not all data controllers.
- 28 The IC agrees that if tiered fees are introduced there should be a penalty for data controllers who knowingly or recklessly provide incorrect information as part of their notification fee assessment. In fact the IC would like the Government to plug an existing gap by introducing a more general offence of knowingly or recklessly providing false information as part of a notification application. It is currently an offence under section 21 of the Data Protection Act for a data controller who should be notified not to be notified. It is also an offence for a data controller who is notified not to exercise all due diligence in notifying the IC of changes to its registrable particulars. Arguably these provisions could be used to prosecute a data controller who knowingly or recklessly provides incorrect information in its initial application. Nevertheless the IC would prefer it to be put beyond doubt that such conduct constitutes a criminal offence.
- 29 The IC points out that the usual formulation describing conduct giving rise to a penalty of this nature is "knowingly or recklessly" rather than "knowingly and deliberately" as suggested in the consultation paper. The words "knowingly" and "deliberately" convey much the same meaning. "Knowingly or recklessly" is for example the formulation used for offences in Section 55 of the Data Protection Act. To prove that a data controller had acted "knowingly and deliberately" would be unreasonably burdensome for the IC and would not capture data controllers who are cavalier as to their responsibilities.

Irish Data Protection Commissioner – Use of Audit and Inspection Powers

The Law

Section 10 (1A) of the Data Protection Acts provide that “The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of (this) Act and to identify any contravention thereof”. Section 24 of the Acts provide for the appointment of “authorised officers ... for the purpose of obtaining any information that is necessary or expedient for the performance by the Commissioner of his functions”. The powers given to such officers include:

- Enter premises, inspect premises and any data therein;
- Inspect, examine operate and test any data equipment therein
- Require any person to disclose data and information
- Inspect and copy information

The powers are deployed flexibly by the Office as part of its tool-kit for achieving better compliance with data protection obligations.

Practice – Routine Audits

At the beginning of each year, a (flexible) programme of audits is drawn up. The list of targets is augmented throughout the year based on information coming to the attention of the Office. The selection criteria include:

- Organisation or sector that has attracted a lot of complaints or media attention
- Large holders of personal data (especially sensitive data)
- Organisation representative of a particular sector
- Balance between public sector and private sector organisations

A letter is sent to the organisation a month or so in advance. The letter announces the intention to carry out the audit on a specified date(s). It sets out the particular issues that the audit team will focus on and names the audit team (the team may sometimes include an outside technical expert). It invites the organisation to submit documentation on its data protection practices.

The audit team analyses any written information provided in advance. On the agreed date (s), it visits the organisation and meets with relevant personnel. Each member of the audit team is an “authorised officer” with the corresponding powers to demand sight of papers etc. It is not normally necessary to formally draw the organisation’s attention to these formal powers - the audit proceeds on an amicable basis.

After the Audit, the Office drafts a report which includes any recommendations for improving data protection practices in the organisation. The draft is sent to the organisation for comment. When these have been received, a final report is drawn

up which is sent to the organisation. The report may include agreed follow-up action by the Office.

In general, those organisations selected welcome the fact of the audit taking place. Only in very rare cases is any resistance encountered either before or during the audit. Sometimes organisations approach the Office seeking an audit. We assume they are driven by a desire to demonstrate compliance for business reasons. Unless such an audit fitted into the audit programme, it would not be undertaken due to a need to focus resources on the areas of concern to the Office.

“Aggressive” Inspections

Routine audits are the norm. Occasionally, the Office may carry out more aggressive inspections of particular data controllers. These are carried out with little or no advance warning. They are usually intended to target contraventions of the Acts for which we already have evidence. Such inspections were carried out in 2007 to gather the evidence which formed the basis for prosecutions under the Electronic Communications Regulations (organisations sending SMS “spam”).

Assessment

Audit and inspection powers are an important part of the Office’s tool-kit. They are deployed strategically to bring about improvements in data protection practice in different sectors.

The knowledge that a statutory audit is to be conducted guarantees senior management attention in an organisation. Organisations are usually ready to acknowledge areas for improvement and to agree to implement necessary measures. Many organisations – once they are assured of the approach – welcome the audit.

A good example of flexible deployment of the tools is in the insurance sector. In 2006/7, media reports suggested that insurance companies were gaining illegal access to information from the Garda Síochána (Police) and from the Department of Social and Family Affairs (DSFA) via private investigators. Targeted audits of a number of insurance companies confirmed this suspicion. An inspection of the DSFA suggested serious deficiencies in the quality of data security.

The net upshot was a package of agreed measures. The Garda accelerated consideration of a draft Code of Practice which had been under discussion with the Office – this was approved in 2007. The same happened with the insurance sector – an agreed Code is imminent. At government level, a high-level review of data security was commissioned which is leading to significant improvements throughout the public sector.

All of the organisations concerned are aware that any further lapses are likely to attract further attention from the Office (and further bad publicity – a key driver of improved practice).

Attachments

- Extract from 2007 Annual Reports describing audit and inspection-linked activity
- Draft Audit Letter

*Office of the Data Protection Commissioner
Portarlinton
28 July 2008*

2007 ANNUAL REPORT (EXTRACTS: AUDITS AND INSPECTIONS)

Over the past year our helpdesk has responded to approximately 20,000 phone enquiries, to number of contacts by post. This large number of queries is partly a result of effective education and awareness-raising exercises and increasing numbers of audits and inspections.

In the summer of 2007, my Office undertook 'raids' of a number of companies engaged in the mobile text marketing sector. These snap inspections came in response to the large number of complaints received in my Office in relation to those companies and as part of my strategy to use my full powers to tackle the problem of unsolicited text messages. As follow-up to the 'raids', my Office is currently bringing prosecutions against those companies that have sent, or allowed to be sent, unsolicited communications to subscribers or that have otherwise failed to comply with their obligations to respect the privacy of individuals..

....

My Office will conduct more 'raids' as necessary in 2008. However I am hopeful that the demonstration set by the 'raids' and the prosecutions currently in train will have a significant deterrent effect on those in the sector who do not comply with their legal obligations. In recent months we have seen evidence of such a trend in the form of a marked decrease in the number of complaints to my Office in relation to this sector. The commercial activities of the premium rate text-messaging sector are perfectly legitimate; our concern (and that of RegTel) is simply to ensure that customers are treated fairly and in accordance with the law governing the sector.

.....

I am empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches. Such audits are supplementary to investigations carried out in response to specific complaints. They differ from the 'raids' undertaken to address unsolicited text messaging (discussed above) in that the timing of audits is usually agreed with the data controller in advance. This kind of inspection is intended to assist the data controller in ensuring that their data protection systems are effective and comprehensive. Priorities for such audits Are set taking account of complaints and enquiries to the Office. During 2007 my Office continued to adopt a proactive role in this regard. In the course of the year, twelve comprehensive audits were carried out. Those audited were:

Aer Lingus
Hays Recruitment
New Ireland Assurance
Quinn Direct
Axa Insurance
Hibernian General Insurance
EBS
Carlow Credit Union
Cavan County Council
University of Limerick
The Homeless Agency
Nursing Home Repayment Scheme

Maple House Emergency Hostel

As in previous years, my inspection teams found that there is a reasonably good awareness of, and compliance with, data protection principles in the organisations that were inspected. Recommendations were made in a number of cases. I am pleased to report that the data controllers concerned were willing to put procedures in place, where suggested, to ensure that they met their data protection responsibilities in full. In addition to the privacy audits, my Office continued with its program of random inspections following the allegations made about the mortgage brokerage and estate agent sectors on the Prime Time Investigates TV programme of December, 2006. As mentioned in my eighteenth Annual Report, my findings indicated a lack of knowledge among mortgage intermediaries in relation to the full extent of their responsibilities under the Acts. I am pleased that our ongoing liaison with the Financial Regulator and with the sector generally has produced positive results in this regard. I would like to thank all of the organisations audited and inspected throughout the year for their cooperation. I believe such privacy audits and inspections are a very valuable tool for improving compliance with data protection principles.

.....

The issue of inappropriate access to information held by the public sector gave rise to increasing concern during 2007. The principal concern arose in relation to allegations that information held on all of us by the Garda Síochána (police) and by the Department of Social & Family Affairs was being routinely accessed by private investigators on behalf of insurance companies engaged in assessing claims. As part of my response I investigated the specific allegations made in relation to insurance companies. I was satisfied that there was sufficient evidence to indicate that private investigators were indeed granted inappropriate access to personal data. To deal with this issue I prioritised the codes of practice which were already under discussion with the Gardaí and the insurance sector. The provisions of the codes place an overt focus on accountability for all access to personal data. I also engaged extensively with the Department of Social & Family Affairs in relation to specific information which came to my attention and I found the Department to be responsive. My key concern was that the Department needed to be in a position to stand over the appropriateness of access to personal data in all cases. This requires that access to information should be restricted on a “need-to-know” basis. Furthermore, where access does take place, it must be subject to audit and follow-up if that access gives rise to any concern – in particular, improper disclosure of data. At the beginning of 2008 my Office conducted an intensive audit with the aim of assessing the situation in the Department and making recommendations for improved compliance with data protection requirements. I am hopeful that, through this process of engagement, the Department will be in a better position to meet its obligations. I will continue to liaise closely with it to this end. In addition, my Office will continue its regular programme of external audit of Garda data protection practices.

AUDIT LETTER TO HOSPITAL

Dear,

Section 10(1A) of the Data Protection Act 1988 & 2003 states the following:

"The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof".

[.] Hospital has been selected as part of an ongoing programme of audits of various sectors that this Office is conducting. It is proposed to conduct the inspection with a three person team including *****, Senior Compliance Officer, *****, Investigations Officer and myself. It is expected that a two day on site inspection may be adequate.

The inspection will focus on those areas within the hospital where personal data is held and processed. In particular, the audit will likely cover, *inter alia*, the following:

- Procedures for handling patient files both manual and electronic
- Electronic systems for recording of patient data including the Healthlink system
- Processing of public patient data / private patient data
- Collection and processing of patient data for research purposes
- External access to patient data by non-health professionals, students, etc
- Procedures for exchange of patient data to HSE

Accordingly, it would be of assistance if personnel with key knowledge of these areas were made available to us during the audit.

The purpose of the inspection is to identify any contraventions of the Acts and to request remedial action where appropriate. To this end, an inspection report will be issued following the inspection. A follow-up inspection may be necessary in order to establish what action has been taken to implement the recommendations (if any) of the report.

The inspection should be seen as an aid to [the] Hospital in ensuring that its data processing operations are conducted in compliance with the provisions of the Act and it is our intention that it will be conducted in a co-operative and hopefully helpful manner. The inspection can also provide an opportunity for any questions or issues to be raised in relation to data protection.

In terms of ensuring the best outcome from the inspection, I am enclosing part 6 of the National Hospitals Office Code of Practice for Healthcare Records Management which examines records management, audit and self audit in the context of healthcare records management. It would be of huge benefit for the orderly conduct of the audit itself if the hospital was able to utilise the audit tool in advance of the audit and provide this Office with a copy of the results.

I am also enclosing this Office's Data Protection Guidelines on research in the Health Sector which will give some insight in terms of the likely approach in this area on the audit.

It is proposed to commence the inspection on, starting at 10am, resuming again at 10am the following day. In advance of the inspection, I would be grateful if you would forward any appropriate documentation relating to the areas under inspection, procedural documents relating to data handling and written training materials. All such documentation should be supplied to me no later than

As it is not the Commissioner's intention to disrupt the operation of your business, I would invite you to contact me to discuss any aspects of the proposed inspection.

Yours sincerely,

.....
Senior Compliance Officer

13 February, 2008