The Information Commissioner's response to the Ministry of Justice's call for evidence on the current data protection legislative framework.

Introduction

The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000. The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The Commissioner's response to this consultation is primarily based on the practical experience he has gained in regulating compliance with the DPA.

The Commissioner welcomes the opportunity to take part in the Ministry of Justice's call for evidence on the current data protection legislative framework. The Commissioner has been very active in this area over the last 18 months, with the publication of the RAND Europe review of the Data Protection Directive[1], which was commissioned by the ICO, through to the Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to the protection of personal data[2]. He was also involved in the Article 29 Data Protection Working Party's joint contribution to the same consultation[3].

Each of these contributions to the debate highlighted a number of aspects of Directive 95/46/EC[4] (the EU Directive) which the Information Commissioner considers need to be addressed to make any future legislative framework for the protection of personal data more effective. This response will detail these aspects in full. However, this call for evidence is looking more broadly at the current data protection legislative framework, and so this response will also include comment on the UK Data Protection Act 1998, as well as other relevant legislation that has a

[1] Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

[2] Available at: http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/public_authorities/ico_uk_en.pdf

[3] Available at: http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/public_authorities/art29_wp_and_wppj_en.pdf

[4] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

substantial effect on the effective protection of personal information in the UK.

The development of increasingly sophisticated information systems, mass information sharing and the online collection of personal information mean that data protection law is more relevant, and more needed, than ever. Not only is personal information shared more often, and in greater volumes, than ever before, but the potential for inadequate information handling systems and practices to have far-reaching consequences has also increased dramatically, as evidenced by the HMRC incident in 2007 and by other high-profile data security breaches.

The level of complaints and enquiries made to ICO goes up all the time[5]. This suggests that individuals and businesses are more aware of information rights issues. This, in turn, suggests that the law is becoming more, not less, relevant to personal and corporate life.

Individual rights in this field are becoming ever more important. ICO research shows that individuals increasingly feel they have lost control of their personal information[6]. In this environment the right of subject access, as well as the right to receive broader information about the data controller and the purposes for which personal data is used, the right to stop processing that may cause damage or distress, the right to stop direct marketing, the right to compensation and the right to have inaccurate personal information rectified are all hugely important.

The ICO has commissioned a number of research reports, qualitative, quantitative and deliberative, over the 10 years since the commencement of the DPA. These reports are publicly available and provide a solid evidence base on the operation of both the DPA and the EU Directive on Data Protection. Many of them are referred to directly in this evidence.

General

Question 1. What are your views on the current Data Protection Act and the European Directive upon which it is based? Do you think they provide sufficient protection in the processing of personal data? Do you have evidence to support your views?

The data protection legislative framework has been a success in raising standards of data protection. However, the Commissioner has no doubt that data protection law could be improved so that it works better in practice, giving individuals an improved set of rights and protections whilst providing greater clarity and reducing unwarranted burdens for data controllers.

[5] See the ICO Annual Report 2009/10 for further information about the number and nature of complaints.
[6] See the ICO Annual Track for 2009 and for previous years, available at www.ico.gov.uk

In the Commissioner's opinion, an effective new data protection framework must:

- be clear in its scope, particularly in the context of new forms of individual identification;
- protect the rights and freedoms of individuals whilst permitting the free flow of data;
- place clear responsibility and accountability on those processing personal data, throughout the information life cycle;
- ensure obligations for those processing personal data are focused on processing that poses genuine risk to individuals or society, rather than focusing on particular categories of data; and
- give individuals clear, effective rights and simple, cost-effective means of exercising them.

The Commissioner hopes that this consultation exercise will eventually result in the development of data protection law that has these features.

The key points that the Information Commissioner wishes to make as part of his submission are as follows. This is not an exhaustive list, nor are the points ranked in any particular order. Other points are dealt with in response to specific questions later in the document.

The data protection principles - The current data protection principles are sound and should be maintained. They represent the fundamentals of good data protection practice. They have generally stood the test of time and are respected within Europe and beyond. They are becoming increasingly familiar and well understood. Any fundamental revision of the principles would be likely to cause confusion and would undermine the historical continuity of data protection law and ultimately its effectiveness. The Commissioner does, however, propose additional requirements which an updated legislative framework should mandate.

Scope - Any new legislative framework should continue to apply to both direct and indirect forms of identification. However, there is evidence of considerable uncertainty in the practical application of the current law to information that identifies people indirectly. This issue and examples of the problems it raises are dealt with in more detail later in this document. A new Directive should open the way for a more realistic treatment of this sort of information. For example, it might require the security principle to apply to all forms of personal data, but acknowledge the practical difficulty involved in obtaining consent for the processing of, or the granting of subject access to, some information that indentifies individuals indirectly. A simple 'all or nothing' approach to data protection requirements no longer suffices, given the variety of information that can now fall within the definition of personal data. The requirements should be more clearly linked to the risk to individual privacy.

A second aspect of the scope of the legislation is that in the UK we have gone further than the current EU Directive requires in applying the UK DPA to "ex-third pillar" bodies, such as law enforcement agencies and national security bodies, albeit with appropriate exemptions. Any new legislative framework at EU level will be brought forward in the context of

the Lisbon Agreement, and should apply to ex-third pillar bodies. The UK experience of applying data protection law to these bodies will be invaluable in discussions on any new legislative framework.

Privacy by design - The principle of privacy by design is implicit in the existing data protection principles - for example, the requirement that personal data shall not be excessive. However, an explicit privacy by design requirement would give a clear message to those designing, procuring and operating information systems that the processing of personal data must be done in the most privacy friendly way practicable.

Transparency and consent - The relationship between these two aspects of fairness can be confusing. An emphasis on consent rather than transparency, or vice versa, can give a very different complexion to data protection regimes across Europe. It can confuse individuals and can cause great practical uncertainty for data controllers. A new legislative framework should give a clearer indication of when consent is needed to legitimise the processing of personal data, and when it is sufficient for individuals to be merely aware that the processing is taking place. Consent should only be used to legitimise processing where individuals have genuinely free choice.

Data controllers and data processors - A simple distinction between a data controller and a data processor no longer fully reflects the complicated relationships that can exist between organisations processing personal data. Any new legal framework must deal more realistically with collaborative nature of modern business and service delivery. In particular, it could open the way for a more collective form of responsibility, extending to all the parties involved in the processing and remaining in place throughout the information life cycle.

International transfers - This is one of the aspects of the EU Directive that most needs to be amended to deal more realistically with current and future international data-flows. A future framework should focus much more on risk assessment by the exporting data controller and should be clearer about data controllers' responsibility, wherever they choose to process personal data. The Commissioner has doubts about a concept of adequacy based substantially on the nature of the law in place in a particular territory. Adequacy should be assessed more in relation to the specific circumstances of the transfer and less on the adequacy or otherwise of the law of the country the recipient is established in.

Sensitive data - The current distinction between sensitive and non-sensitive categories of personal data does not work well in practice. The Directive's special categories of data may not match what individuals themselves consider to be 'sensitive' – for example their financial status or geo-location data about them. However, rather than creating more categories of sensitive data, The Commissioner suggests a more flexible and contextual concept of sensitivity, which could, depending on the circumstances, extend to any type of personal data.

Personal or household activity - A better understanding is needed of what comes within the scope of purely personal or household activity. This is becoming an acute practical problem given private individuals' capacity to process personal data on the internet and to make it widely available to other individuals, for example through social networking services. There are also questions about how far the current exemption that relates to journalism or the purposes of literary or artistic expression can be applied to the activities of private individuals on the internet. There are also significant practical consequences for data protection authorities in terms of the extent to which any new legislative framework may require them to regulate private individuals' online behaviour.

Complexity - The perceived complexity of the data protection legislative framework is sometimes used as an excuse for not complying with data protection law by organisations. When it comes to reforming the EU Directive and the DPA, there needs to be a focus not only on 'updating' but on achieving greater clarity of purpose and presentation. It must be emphasised that the ICO does not consider the fundamentals of data protection law to be complex, but there are several areas of concern where both the EU Directive and the DPA lack clarity and certainty, and it is these areas that need to be addressed.

Any new legislative framework should also focus more on outcomes for individuals, and be based less around bureaucratic processes. Greater use of standards and/or an accountability requirement (as described below) might facilitate this.

Accountability -The Information Commissioner would like to see a new, general requirement of accountability introduced. This would reinforce the responsibility of data controllers for ensuring that personal information is properly protected in practice by requiring them to:

- take appropriate and effective measures to implement data protection principles; and
- be able to demonstrate, on request, that such measures have been taken.

The requirement would not impose any additional burden on data controllers that take their responsibilities seriously, but would emphasise, on the face of the legislation, that data controllers have to take concrete measures to deliver effective data protection in practice. It would, through the transparency element, also assist DP authorities in targeting their activities on areas of genuine DP risk.

An accountability requirement would have to be scalable to the size of the organisation concerned and the risks of the processing of personal data they perform, so as not to impose any further unwarranted obligations on data controllers. Whilst a large multinational might be expected to have measures in place such as relevant policies and procedures, a data protection official, privacy impact assessments and training programmes, an SME would not necessarily be expected to do any more than be able to explain the steps it has taken to identify and address any risks its business poses to the privacy of personal information. Accountability

already features in DP regimes outside Europe including the OECD privacy guidelines and the APEC privacy framework. Its introduction as a principle in the EU legal framework would promote global harmonisation of DP requirements and could contribute to reducing the administrative burden imposed by the current rules on international data transfers.

Freedom of information - Another unintended consequence of the legislation comes not from the legislation itself but from the introduction of the Freedom of Information Act 2000 (FOIA), which post dates the introduction of the DPA. The introduction of the FOIA and subsequent decisions and judgments by the ICO, the Tribunal and Higher Courts have dramatically increased the volume of case law related to the areas where there is an interaction between the DPA and the FOIA. In particular this involves the application of the first data protection principle. This reflects a wider issue of access rights to information or documents across the EU and the potential impact on individual privacy.

There are a number of issues around how the legislation interacts. The ICO has identified the following matters as key points of concern.

- Requests made under the FOIA for third party sensitive personal information have led to scenarios where it would be fair to disclose information and a schedule 2 condition of the DPA can be met, but no condition for processing sensitive personal data can be found. This leads to non-disclosure on technical legal grounds, even though information could be disclosed without any undue impact on privacy. Case law developed by the Tribunal has focused closely on technical application of the conditions for processing personal data.
- Anonymisation - issues considered in Freedom of Information decisions/judgments have highlighted difficulties in interpreting the definition of personal data in conjunction with recital 26 of the Directive and in establishing suitable tests for deciding when information is "anonymised".
- Applicants will often make "hybrid requests" for their own personal information and other information held by public bodies, at the same time. Applicants are often confused by the different adjudicatory roles the ICO has under section 50 FOIA and section 42 DPA.

The ICO would like to see any new data protection regime more closely aligned with the FOIA regime, with simpler and clearer mechanisms for balancing the potentially competing interests of personal privacy and access to information.

Definitions

Question 2. What are your views of the definition of "personal data", as set out in the Directive and the DPA?

There is a lack of clarity in the current data protection legislative framework in the UK in determining what is "personal data". This arises in part because the wording of the UK DPA is different to that in the EU DP

Directive. Whilst both definitions can be interpreted as meaning essentially the same thing, case law and the advances in technology have led to confusion about what the definitions mean in practice, and the data that comes within their scope. Any revision of the current legislative framework should be seen as an opportunity to remove this area of doubt and provide data controllers with greater legal certainty as to what constitutes personal data.

In the Commissioner's opinion, a future framework must deal better with the new forms of identification that are coming into being all the time, particularly in the online environment. It is clear that information such as IP logs held by search engines are being used to identify individuals and to take action affecting them, in contexts ranging from behavioural advertising to digital rights management or national security. It is clear that data protection ought to apply to this sort of information. However, we have to be realistic about how such information is treated under the law, what standards we expect those processing it to reach and what outcomes we are seeking for the individual. Whilst we may want this information to be kept secure and protected from inappropriate disclosure, it may be impossible in practice to grant conventional subject access to it or to expect individuals to consent to its processing. The Commissioner hopes that a future framework will treat this sort of information more realistically, perhaps recognising that a simple 'all or nothing' approach to the application of data protection requirements no longer suffices, given the breadth of information now falling within the definition of personal data.

A further consequence of the legislative framework is that sometimes the interpretation of what is, or is not, "personal data" for the purposes of the DPA has led to an undermining of certain rights and protections afforded to the individual. For example, there is some anecdotal evidence of organisations deliberately using filing systems that are organised by address, or some other taxonomy, and trying to claim that the information is no longer "personal data" and thus not liable to be released in response to subject access requests, or even that they do not have to comply with the broader provisions of the legislative framework.

Question 3. What evidence can you provide to suggest that this definition should be made broader or narrower?

The Information Commissioner is not of the opinion that the definition necessarily needs to be broader or narrower, but rather that it needs to be more relevant to modern technologies and the practical realities of processing personal data held in both automated and manual filing systems. The definition also needs to be much clearer. The lack of legal certainty in the definition is, in itself, becoming a burden for business.

When the EU Directive was first drafted, it might have been reasonable to presume that only paper records held in a system of similar sophistication to computerised records should be covered by the legislative framework. The development of technology has meant that this link between the sophistication of manual records and computerised records is no longer

realistic. In particular, powerful search technology makes issues of structure increasingly irrelevant – huge collections of random, unstructured information can be searched very quickly and thoroughly.

Similarly the advance of technology has led to many different levels of "identifiability" of the individual, both directly and indirectly. Any new legislative framework must be more relevant and treat certain types of "personal data" more realistically.

For instance, pharmaceutical companies hold millions of records relating to individuals but in such a way that obvious identifiers have been stripped away. Indeed, linking the record or the sample back to the individual to whom it relates would not be a trivial matter and would involve unpicking various coding processes. The Information Commissioner does not believe that the definitions should leave data held in this way outside the legislative framework but clearly such data require different levels of protection from other personal data from which the data subject is more easily identified.

At the same time, true anonymisation of personal data is becoming more difficult, particularly with the increase in publicly available data sets. As more and more information is made publicly available, there must be a more nuanced approach to what constitutes "personal data" and what level of protection such data is afforded. Where data is released into the public domain in a truly anonymised form, data controllers are still required to justify the disclosure in the same manner as if they were releasing non-anonymised, sensitive personal data. This involves establishing a legal basis for the disclosure, along with a processing condition for sensitive personal data[7]. Considering the data is anonymised, such a construction is excessive, creating a barrier to transparency without any corresponding additional protection for the personal data concerned.

Question 4. What are your experiences in determining whether particular information falls within this definition?

It is sometimes difficult to determine whether particular information falls within the definition of 'personal data'. At one end of the spectrum, it is fairly easy to apply the definition, for example in respect of information recorded against 'traditional' personal identifiers, such as individuals' names and addresses. However, the Information Commissioner is being asked to deal increasingly with information that, though it is not linked to a 'traditional' identifier, to some extent relates to a particular individual's property, activity or other attribute. For example, the Commissioner receives many enquiries from people trying to access information about the houses they live in. Where this information is held in street order by a local authority, for example, it can be unclear whether an individual

[7] For an example of this see the Decision promulgated by the Information Tribunal on 15 October 2009 between the Department of Health and the Information Commissioner and the Pro Life Alliance.

occupying a house has a right of subject access to it under section 7 of the DPA.

Situations like this cause significant practical difficulty for individuals, data controllers and the regulator. This should be addressed as part of any new legislative framework but with legal certainty that all information that relates to individuals is covered by the law.

Question 5. What evidence can you provide about whether biometric personal data should be included within the definition of "sensitive personal data"?

The term 'biometric personal data' is perhaps misleading. Biometry involves capturing a piece of biological information, such as a measurement of a person's facial features, and using an algorithm to convert this into a biometric – put simply a set of numbers. A reader is then used to determine whether biological information presented to it on a subsequent occasion corresponds with the biometric already held in a database. This process is used to determine whether a person should be allowed to enter a building, for example. Therefore any new legislative framework needs to draw a distinction between the raw biological data from which a biometric is derived, and the biometric itself; the terms are sometimes used interchangeably.

The Information Commissioner is not of the opinion that a physical or biological characteristic should necessarily be included within the definition of 'sensitive personal data'. Nor does he consider that the biometric itself should necessarily be considered 'sensitive'. This is because of the wide range of biometric systems in existence and their varying effect on individuals. For example, the Commissioner would not consider the processing of a basic biometric derived from a finger-print to determine whether someone is entitled to borrow a book from a library to be a sensitive in any real sense. However, the situation may be different where a complex fingerprint biometric system is being used to verify a person's benefit claim or determine whether they are allowed to enter a particular country. This supports the Commissioner's view, expressed elsewhere in this document, that sensitivity arises from the overall nature of the processing operation, particularly its actual or potential effect on individuals, rather than just the nature of the information being processed.

Question 6. If as a data controller you process biometric data, do you process it in line with Schedule 3 of the DPA which imposes an additional set of conditions?

The Information Commissioner has some doubt about the legal framework that involves the need to satisfy a condition to legitimise the processing of personal data, and an additional condition where sensitive personal data are involved. He believes that this can result in the artificial justification or restriction of otherwise unobjectionable processing and offers little meaningful protection to individuals. Indeed the predecessor to the current DPA, the Data Protection Act 1984, did not contain special

provisions governing the processing of sensitive personal data. In practice this did not stand in the way of the proper protection of genuinely sensitive data but provided more flexibility for business and the ICO in the way this was delivered.

Again, given the problem of defining biometric data, and determining whether it is 'sensitive', it is difficult to say whether data controllers are required to satisfy a Schedule 3 condition and if so, whether they are able to do so. For ICO's own part, we do process biometric data, for example copies of signatures on electronic documents and staff members' photographs for security purposes. We would find it difficult to satisfy a Schedule 3 condition in order to legitimise the processing of this data. However, we do not believe that a failure to categorise the data in question as 'sensitive' prejudices the rights of ICO staff members or those who come into contact with our organisation. We suspect that many other data controllers would share our experience.

Question 7. Are there any other types of personal data that should be included? If so, please provide your reasons why they should be classed as "sensitive personal data"?

The treatment of "sensitive" or "special categories" of personal data is an area of the legislative framework that the Commissioner considers does not work well in practice. The categorisation was clearly an attempt to afford special protection to the sorts of data that could have the most negative impact on individuals if used inappropriately. For example, information about trade union membership has been used against individuals living under the various totalitarian regimes that have existed in Europe. Although the rationale for categorising certain types of data as "sensitive" is easy to understand, there are several practical problems.

First, the Directive's special categories of data may not match what individuals themselves consider to be 'sensitive'. To use the example above, many trade unionists living in relatively stable, democratic societies probably wouldn't consider information about their membership to be sensitive, or believe that its existence leaves them open to particular threats, despite this information being misused in certain circumstances, such as the Consulting Association's vetting database[8]. However, many individuals would probably consider their personal finances or, in some circumstances, information about their location to be very sensitive. This shows that there can be a mismatch between what the law says and what people believe to be "sensitive". The difficulty with defining a set list of categories of what constitutes "sensitive personal data" is that it is a very subjective judgement, based entirely on the cultural or social mores at the time. This can not only lead to certain categories of data which might otherwise be considered sensitive falling outside the definition. There is also the danger that the list may be different in jurisdictions outside the

[8] For further information, see the enforcement notice issued by the Information Commissioner to the Consulting Association, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/notices/tca_enforcement_notice.pdf

EU, leading to multinationals to cope with different lists of sensitive personal data in a range of countries.

Just one example of this can be found in a draft discussion Bill that was put forward in the USA earlier this year[9]. This Bill defined "sensitive information" by a list of categories, some of which overlapped with those categories in the current EU legislative framework. However, other categories, such as precise geolocation information and financial data, were counted as "sensitive" (as an aside, biometric data was not considered to be "sensitive" in the draft Bill). This demonstrates the difficulty in defining "sensitive personal data" as a list of categories, as opposed to defining it against the impact, or potential impact, of the processing of the data has on the individual.

Second, there is the issue of context. As it stands, certain types of data are deemed to be special regardless of what the precise information is, who it is held by or what it is used for. Clearly, many individuals would consider their health data to be sensitive, but is a record kept in a manager's file recording that an employee was absent from work because he or she had a cold particularly sensitive in any real sense?

The way the EU Directive is structured means that where special categories of data are involved, their processing is prohibited unless one of a number of conditions applies. This has led to cases where legislation has had to be created in Member States to provide an explicit legal basis for carrying out otherwise unobjectionable processing. This has happened several times in the UK, and, we gather, in other countries too. The Commissioner's view is that the rigid categorisation of special categories of data is not an effective way to allow acceptable processing but prohibit the unacceptable. We need a more flexible and contextual conception of sensitivity, which could, depending on the circumstances, extend to any type of personal data.

The Information Commissioner suggests a definition based on the concept that information is sensitive if its processing could have an especially adverse or discriminatory effect on particular individuals, groups of individuals or on society more widely. This definition might state that information is sensitive if the processing of that information would have the potential to cause individuals or significant damage or distress. Such an approach would allow for flexibility in different contexts, so that real protection is given where it matters most. In practice, it could mean that the current list of special data categories remains largely valid, but it would allow for personal data not currently in the list to be better protected, for example financial data or location data. Or, more radically, the distinctions between special categories and ordinary data could be removed from the new framework, with emphasis instead on the risk that particular processing poses in particular circumstances.

---

[9] A Draft of a Privacy Bill was presented before the House of Representatives in the USA on 4 May 2010 by US Representatives Rick Boucher and Cliff Stearns. A full draft of the Privacy Bill can be found at http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf

It is important to give a message to data controllers that a simply binary (special categories – the rest) approach is not good enough, and they must consider the context in which they hold information and the risk this poses to individuals. In the context of a revised legal framework national data protection authorities or EU-level bodies, such as the Article 29 WP, could produce guidance with examples that could help organisations to assess genuine sensitivity in various contexts. Regulation of misuse of "sensitive" data in this way would be in line with the Information Commissioner's current risk based approach to regulation.

Question 8. Do you have any evidence to suggest that the definitions of "data controller" and "data processor" as set out in the DPA and the Directive have led to confusion or misunderstandings over responsibilities?

There can be a lack of clarity and certainty in determining which is the "data controller" and which is the "data processor" in relationships between organisations that process personal information. The complexity of modern business relationships means that there are endless possibilities and the question of who takes ultimate responsibility for ensuring that personal information is processed in accordance with the law is often opaque. This is not helped by very general definitions as to what constitutes a "controller" or "processor" under the DPA, nor by the concepts of "joint controllers" or "controllers in common", two concepts that are introduced in the DPA but which are not defined.

Another area of confusion is what is meant by determining the "manner of processing" in the UK when the EU Directive refers to the "means". The Commissioner sees the revision of the legislative framework as an opportunity to remove this uncertainty.

With regard to definitions in the EU Directive, it is clear that a simple distinction between a data controller and a data processor no longer reflects the complicated relationships that exist between organisations processing personal data. The definitions of "controller" and "processor" in Article 2 of the Directive assume that there is always a clear distinction between those who determine the means and purpose of the processing and those who process on behalf of the controller. The definitions assume that a processor is an essentially passive entity, acting on behalf of a controller, with no independent influence over the way the processing takes place. This does not reflect the reality of current business practice where an organisation that at first sight appears to be a data processor – typically a sub-contractor – may exercise considerable influence over the way the processing takes place and may, in many respects, act as a data controller. This situation is made all the more difficult because subcontractors may outsource certain aspects of their work to other subcontractors. This can make it difficult to establish responsibility, for example, in enforcement cases. An explicit accountability principle might help deal with controller-processor relationships that are difficult to define.

The Information Commissioner supports the work the Article 29 Working Party has done[10] to address these questions under the current legal framework. This underlines the importance of making sure the future legal framework is able to respond to the reality of how organisations and communication systems work today.

One example that illustrates the difficulty has been the data controllership of the Police National Computer (PNC). Individual police services decide what data is held about individuals on the PNC and are considered to be data controllers in common. However, decisions on the operation of the system as a whole, for example who is allowed to access PNC data, are taken centrally. It has been difficult to establish who the central data controllers are and ultimately who the ICO would take action against in the event of significant non-compliance. The Association of Chief Police Officers (ACPO) in particular has been reluctant to accept this responsibility.

Another example is the National Health Service (NHS). Despite its name, in reality "the NHS" is not a single organisation. It is made up of numerous disparate and separately managed regional and local units such as Hospitals, Primary Care Trusts and GP Practices. GP Practices, in particular, are not part of the centrally managed system and GPs are individual contractors.

All of these units are data controllers for the personal data of patients they deal with but they do not necessarily work as joint data controllers or data controllers in common. The complex structure of the NHS and the development of electronic health records which has given clinicians and managers' wider access to patients' personal data across the NHS can cause difficulties in establishing which unit is the data controller and has the responsibility for a particular data protection matter.

In the private sector it is also true that the standard view that a data controller might use the services of one or a few 'dumb' processors while retaining responsibility over and making choices about all processing operations is out of date. Financial services companies, for example, may use hundreds of data processors and may cede a great deal of responsibility over how personal data are disposed of or how certain customers are contacted to those processors. They may also use data processors who are legally separate entities but who are also part of the same wider group of companies subject to the same 'internal' corporate rules. These are far removed from the relationships described by the definitions and the interpretation of the seventh data protection principle, yet are treated in the same way by the legal framework.

A final example is in the use of third parties in behavioural advertising. Adverts are placed by an advertising network to which a publisher is affiliated. The publisher has chosen the adverts based on which other affiliated websites have been visited by the user. This information is linked

[10] Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

by an identifying cookie on the user's machine, which can be accessed by the network but not the publisher. In this arrangement, identifying who is the "data controller" is far from clear. This complex arrangement highlights confusion for all parties, especially the consumer who may simply be trying to exercise their rights.

Question 9. Do you have any evidence to suggest that the separation of roles has assisted in establishing responsibilities amongst parties handling personal data?

As stated above, the Information Commissioner considers that the lack of clarity of roles has caused confusion and misunderstanding without necessarily helping to establish where responsibility ought to properly lie in modern business relationships. However, organisations appear generally capable of working together to protect personal data even though they may be unclear as to their own status as data controller and/or processor. In addition, the ICO's own guidance stresses the importance of organisations establishing who has responsibility for which aspects of the processing of personal data, through contracts or similar mechanisms.

Question 10. Is there evidence that an alternative approach to these roles and responsibilities would be beneficial?

Rather than trying to keep rigid definitions, more effective data protection could be achieved if any new legal framework clearly identifies that between them the persons responsible for the various aspects of the processing of data retain responsibility throughout the information life cycle. In principle responsibility could be assigned to the organisation, or organisations, that initiate the processing – typically by collecting the information - but anyone processing personal data at any stage of the information life cycle would carry responsibility for dealing with it properly and securely, and be accountable for their own aspect of the processing. This could mean being accountable to whoever initiated the processing; to individuals; to regulators; or all three. There are also messages here that must be communicated to data controllers, in terms of developing clear lines of mutual responsibility where a number of organisations may be jointly or commonly responsible for the processing of personal data.

Question 11. Do you have evidence that demonstrates that these definitions are helpful?

Clearly some definitions are needed. The existing definitions were more relevant when they were introduced and have been helpful in establishing lines of responsibility in some cases. The point is that the definitions would be more helpful if they were drafted differently and are becoming increasingly difficult to apply to modern processing operations.

Data subject's rights

Question 12. Can you provide evidence to suggest that organisations are or are not complying with their subject access request obligations?

As the regulator for the DPA the Information Commissioner receives many complaints about subject access requests being refused – 28% of the 33,234 written requests for advice/complaints received in 2009/10 concerned subject access requests. It must though be pointed out that often any dispute is not because the data controller has failed to comply with the request *per se*, but that the requested information has been withheld under one of the grounds under Part IV of the DPA (exemptions)[11].

Causes of dispute over whether an individual is entitled to the information requested include questions such as whether information about other individuals might be disclosed as a result and whether it is reasonable to disclose such information without the consent of those other individuals. In some cases, as detailed above, there is confusion as to whether or not the information being requested is actually personal data. Finally some organisations are not aware of the individual right of subject access[12]. In the ICO's experience of dealing with complaints, we find that simply making organisations aware of their obligations is often enough to ensure access is provided.

Question 13. Do businesses have any evidence to suggest that this obligation is too burdensome?

The ICO does not have specific evidence about subject access. In the context of burdens on business though, the ICO's annual track research[13] for organisations in 2009 showed sustained positivity and appreciation of the role of the DPA more generally. 94% of organisations agreed that the DPA is needed. In terms of whether the DPA presents additional burdens, our annual track showed on 16% of organisations who responded felt the DPA means extra work and only 7% feel that the DPA is itself a burden.

Unlike in previous years, the Annual Track research for 2009 showed there had been a decrease in the number of subject access requests over the past 12 months in the private sector. 48% of organisations have received at least one request, compared to 53% in 2008.

---

[11] For a full breakdown of complaints about subject access, see the Information Commissioner's Annual Report for 2009/10.

[12] The ICO Annual Track research for organisations showed unprompted awareness of individuals' *right to see information* has decreased by 10% (from 82% to 72%) since 2008. However, it is still higher than levels recorded between 2003 and 2006. This decline in unprompted awareness has been driven by smaller private organisations (-15%) and larger public organisations (-13%). The decline across public and private overall was equal.

[13] The ICO Annual Track research for individuals and organisations are both available at http://www.ico.gov.uk/about_us/research/corporate.aspx

Numbers of requests do seem to be in proportion to the size and resources of the organisations concerned. Public sector requests have continued to increase to some extent (for organisations that received between 10-200 requests and 500+ requests). 80% of organisations have received at least one request (compared to 79% in 2008). Large public organisations remain the sector that is most likely to receive a high volume of requests – 36% received more than 50 requests in the last year (this was also the case in 2008), compared with 19% of small-medium organisations in the public sector.

Smaller organisations are, unsurprisingly, more likely to have received no or few requests. Again police forces were likely to receive the highest numbers of requests for personal information.

The Information Commissioner is of the view that many requests for personal information are actually dealt with every day by business as part of their day to day activities. This is seen as essential to good customer or public service. It is only where an organisation is being recalcitrant that the formal rights of subject access needs to be invoked. As with most aspects of regulation, it is only the reluctant organisation, which is not set up to provide information to a data subject, that is likely to find the right of subject access a burden.

A final point is about the purpose of subject access rights. There is some misunderstanding about why subject access rights exist, due partly to comments made in the Courts, about subject access rights existing primarily for the data subject to check whether the information held about him or her is accurate or not. This is not the case and any changes to the legislative framework should not be founded on this assumption.

The right of subject access is a standalone right, around which is central to the data protection legislative framework. It enables individuals not just to check for inaccuracy, but also to be able to understand the full scope of the personal data an organisation holds about them, and to understand the sources and recipients of that data. The right of subject access empowers individuals in their relationships with organisations, enabling them to see if the processing of their personal data is excessive, to check whether information is being held for longer than is necessary and that the purposes for which they have been told the information is processed are the purposes their data is being used for. Being able to request access to information about oneself is absolutely essential if individuals in the information society are to be afforded their rights under Article 8 of the European Convention on Human Rights. Any attempt to attach a specific purpose to this right misunderstands its fundamental importance in the regulatory framework.

Question 14. Approximately how much does it cost your organisation to comply with these requests?

As a data controller as well as a regulator, the ICO deals with subject access requests. Currently we do not calculate the unit costs for handling each subject access request. However, in the last financial year we

received 900 information requests of which 35% had a Data Protection element.

It is worth emphasising that the charging regime for subject access requests was never meant to be a means to recover costs and should not be treated this way now. Rather it is a deterrent to the frivolous request. The cost of responding to subject access requests is a necessary cost for businesses that process personal data as part of their commercial activities.

The Information Commissioner would also highlight that a right of subject access has been on the UK statute books since the Data Protection Act 1984 received Royal Assent. Organisations have had several decades of having to respond to such requests, and should bear this in mind when procuring new systems so that they facilitate compliance. While the Commissioner does have some sympathy with organisations that have to deal with a particularly high number of "vexatious" requests, in general complying with the right of subject access should not be particularly burdensome on those organisations that have put sufficient consideration into procuring information systems and implementing records management processes that help them meet their obligations.

Question 15. Have you experienced a particularly high number of vexatious or repetitive requests? If so, how have you dealt with this?

This is an interesting question, in particular as these are terms more readily associated with the FOIA regime rather than data protection. It is worth pointing out that each access regime has different criteria for deciding whether or not there is an obligation to respond to an information request. There is no provision to refuse subject access requests made under the DPA on the grounds that such requests are "vexatious", unlike under Section 14(1) of FOIA.

There is provision in the UK DPA for data controllers to be released from their obligation to supply a copy of personal data where provision of such a copy would require "disproportionate effort" on the part of the data controller[14]. While there may be some overlap in meaning, this is a very different concept from whether the request for a copy is "vexatious" or not, and highlights the differences between the different information access regimes in the UK. However, it is worth pointing out that while an organisation might be in technical breach of Section 7 of the DPA, it is unlikely that the Information Commissioner would use his enforcement powers where a request was demonstrably "vexatious".

With the range of personal and no-personal information access regimes in the UK and across Europe, it can be confusing for practitioners when faced with requests for information. Perhaps any new data protection legal framework could take these differences into account.

[14] Section 8(2)(a) of the DPA

The ICO as a data controller does not experience a high number of repeated subject access requests. However, if a subject access request is made in the course of an ongoing investigation and where a reasonable period has passed there will be new information to consider and so another request can legitimately be made. The ICO does not gather information as to whether subject access requests it receives are "vexatious" or not as there is no provision for this in the UK DPA.

Question 16. What evidence is there that technology has assisted in complying with subject access requests within the time limit?

The Commissioner believes that much more can be done to harness technology to deliver improved rights for individuals, for example, online access to their personal information. Again, a future framework should do more to update and strengthen individuals' rights, particularly in terms of subject access and the way increasingly complex information systems are explained to the public.

Question 17. Has this reduced the number of employees required and/or time taken to deal with this area of work?

The Information Commissioner is unable to comment on this question.

Question 18. Is there evidence to suggest that the practice of charging fees for subject access requests should be abolished?

Whilst the Information Commissioner is strongly of the view that the fee should not, primarily, be seen as a means to recover costs, he is sympathetic to organisations that argue that a nominal charge for subject access is necessary, particularly for smaller organisations for which complying with subject access rights can be more burdensome. However, the fee should not be raised as this may prove a barrier to individuals asserting their rights, particularly those on lower incomes. In addition, the argument for charging a fee is weakened where there is provision for an individual to go online and access their own records with no administrative expenses for the data controller.

Question 19. Do you have evidence that the £10 fee should be raised or lowered? If so, at what level should this be set?

The Information Commissioner is of the view that the current subject access fees should not be raised. Currently the fee that most data controllers can levy for compliance with subject access requests is £10, with subject access requests for manually held health and education records costing up to £50. Considering the voluminous nature of some of these types of manual records, it is appropriate that data controllers in these areas have the facility to charge more than a £10 flat fee.

However, the Information Commissioner would point out that any charge can be a disincentive to exercising rights of subject access, particularly for those on very low incomes. In this context it should be borne in mind that an individual wanting to track their personal data may have to pay several

fees where data has been shared between different data controllers. It should also be borne in mind that there is no fee for an application to a public authority under the FOIA regime. Should subject access fees be maintained, there could be a provision for these to be waived if the charges are unreasonable based on the individual's financial circumstances.

Question 20. Do you have evidence to support the case for a "sliding scale" approach to subject access request fees?

The Information Commissioner has no evidence to support the case for a sliding scale approach to subject access fees. The Information Commissioner would repeat that he supports the current charging regime, and understands that having the option of making a limited charge for subject access requests is a useful provision for some organisations. However, introducing a more general sliding scale might discourage individuals from asserting their subject access rights, particularly those on very low incomes.

In addition, having a single set fee is in line with better regulation principles, as it provides simplicity and clarity for data controllers who have to discharge their functions. It also provides clarity for individuals. A sliding scale of charges would be likely to add unnecessary. This confusion would lead to greater potential for dispute, precipitating the need for greater regulatory action at greater costs – which again would not be in accordance with the principles of better regulation. For this reason, the Commissioner recommends that the current sliding scale fees regimes for accessible records are also removed under any new legislative framework.

Question 21. Is there evidence to suggest that the rights set out in Part Two of the DPA are used extensively, or under-used?

Our annual track 2009 showed that the right of subject access was the most used right, with 16% of respondents having made a request for information about themselves in the past[15].

Some of the rights are used extensively, such as the right of subject access or the right to prevent direct marketing. Others are widely misunderstood, such as the rights in relation to automated decision making in Section 12 of the DPA and rights to stop processing that causes damage or distress in section 10 of the DPA. Some rights are more limited, such as the rights to the rectification, blocking, erasing or destruction of personal data by application to a court under Section 14 of the DPA[16].

The right to compensation in Section 13 of the DPA appears only to have been used infrequently, but is a valuable right for individuals where they can demonstrate damage as a result of a breach of the data protection principles.

[15] See the ICO Annual Track 2009 for Individuals
[16] See the ICO Annual Track 2009 for Individuals

The Information Commissioner believes it is a fundamental part of better regulation that individuals have easily understood rights. Complexity and misunderstanding create greater burdens on data controllers and make it more difficult for individuals to assert their rights effectively.

Question 22. Is there evidence to suggest that these rights need to be strengthened?

The rights in Part II of the DPA, including an individual's right of access to their own data, can only be enforced directly by an individual through the Courts. This can be a complex, costly and time consuming process. However, if a third party makes an FOIA request for a different individual's personal data, they have a mechanism for asserting that right through the Information Commissioner's Office and Tribunal. While the Information Commissioner may assess likely compliance with the rights under Part II of DPA, his decisions are not binding, and the Tribunal does not have any oversight of these decisions, unless the Commissioner chooses to use his formal enforcement powers. There is an inconsistency here that should be addressed.

As stated in answer to question 21, many of the rights in Part II of DPA are quite complex and difficult to understand and assert effectively. The rights are potentially quite far reaching, but they need to be simplified and there need to be better and more effective processes for asserting them. Rights for individuals need to be simple and directly enforceable. They need to keep step with the way data is processed. For example, giving individuals online access to their records; having simple, free ways to make access or redress requests online; the availability of alternative dispute resolution procedures rather than going to court, and so on. Individuals should have access to effective and readily accessible remedies; it is not enough to tell them to go to court. In addition, there needs to be provision made for quick resolution of complaints within Europe which may boundaries between Member States.

One specific point is in relation to section 56 of DPA, which relates to enforced subject access. The Information Commissioner is still awaiting the coming into force of sections 112, 113 and 115 of the Police Act 1997 to trigger section 56 of the UK DPA.

A final point to make is about to the right to compensation provided under Section 13 of the UK DPA, which is currently only available for "distress" where either damage can also be demonstrated, or where the distress caused is by processing of personal data for the "special purposes". This is not sufficient. The very nature of personal data is such that its loss or misuse is likely to cause distress to data subjects, without necessarily causing them quantifiable damage. This fact is recognised elsewhere in the DPA, for example in relation to the criteria for imposition of a monetary penalty, or in the rights provided to data subjects to prevent processing likely to cause damage or distress. It is important that this inconsistency and deficiency within UK law is addressed so that individuals

can be compensated for any genuine harm they suffer as a result of a breach of the DPA.

The Information Commissioner's view is not expressed in isolation. The Federal Trade Commission of the United States of America has recently stated:

"..many commentators have called upon the Commission to support a more expansive view of privacy harms that goes beyond economic or tangible harms. There are some privacy harms, these participants argued, that pose real threats to consumers – such as exposure about health conditions or sexual orientation – but cannot be assigned a dollar value."[17]

Obligations of data controllers

Question 23. Is there any evidence to support a requirement to notify all or some data breaches to data subjects?

The Information Commissioner supports some form of requirement to notify him about more serious breaches. Although there is currently no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office. The nature of the breach or loss, particularly its actual or potential effect on individuals, can then be considered together with whether the data controller is properly meeting its responsibilities under the DPA. The recent revisions to the ePrivacy Directive 2002/58/EC place an obligation to notify on information society service providers and the Information Commissioner would urge the Government to monitor carefully the implementation of these new rules with a view to assessing the benefits and practicality of widening their application to all data controllers.

In the past the Commissioner has argued that notification of serious security breaches to the Commissioner is an appropriate organisational measure and a matter of good practice in complying with the seventh data protection principle. However, if any new legislative framework is going to introduce an explicit requirement to notify security breaches, this must not be too prescriptive. There should be a sensible definition of what constitutes "serious breaches" on the basis of risk. If all security breaches are to be notified, this could create the potential for huge and disproportionate administrative burdens for both businesses who have to notify breaches regardless of their seriousness, and for the regulator who has to administer those breach notifications. This could divert scarce resources from other, more effective regulatory activity.

The UK has some experience of doing this well. The Information Commissioner has issued guidance on the notification of the most serious

[17] As stated in a Prepared statement of the Federal Trade Commission on Consumer Privacy, before the Committee on Commerce, Science, and Transportation, United States Senate, Washington DC on 27 July 2010.

breaches[18]. In central Government departments and other areas of the public sector, security breaches must be reported in the statement of internal controls and are therefore subject to regular corporate audit procedures[19]. This could be a model that would work well across Europe, with organisations required to record all their breaches but requiring them only to report the most serious ones to the relevant data protection authorities. There could also be a link here to the accountability requirement principle referred to above.

Question 24. What would the additional costs involved be?

The Information Commissioner has no evidence to present about costs of notification of security breaches, but does not see that the costs of notifying the ICO should add significantly to the costs a responsible organisation will face in any event in addressing the consequences of a serious breach. In fact, the Commissioner had to formalise his guidance on the notification of security breaches to his office in response to demand from data controllers who were keen to report appropriate breaches but did not fully understand what the Commissioner considered to constitute a "serious breach" worthy of reporting.

Question 25. Is there any evidence to suggest that data controllers are routinely notifying data subjects where there has been a breach of security?

The Information Commissioner has no evidence to offer here. It is important to note that sometimes notification to data subjects might be disproportionate or present further risks. For example, notifying those involved in criminal proceedings that data has been lost could encourage attempts to identify and intimidate witnesses. As such the Commissioner would not welcome any blanket requirement to notify data subjects as part of a new legislative framework.

However, the Information Commissioner considers that there is a strong case for breach notification where a failure to inform the individuals would leave them open to financial loss or danger, for example.

The Information Commissioner's main consideration is that any new requirement to notify must actually be effective in either protecting individual's interests or in reducing breaches. These are difficult areas to quantify. There are several reports on breach notification to individuals in the United States. Two of note would be the research by Javelin Strategy

[18] Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf

[19] See, for example, paragraph 3 of the Cabinet Office document "Cross Government Actions: Mandatory Minimum Measures", published on 25 June 2008

and Research[20] and "Dos and don'ts of data breach and information security policy"[21].

Question 26. Do you have evidence to suggest that other forms of processing should also be exempt from notification to the ICO?

The DPA provides an exemption from notification for some data controllers. Exemptions are possible for the following.

- Data controllers who only process personal data for:
  - staff administration (including payroll);
  - advertising, marketing and public relations (in connection with their own business activity); and
  - accounts and records.
- Some not-for-profit organisations.
- Judicial functions.
- Processing information for personal, family or household affairs (including recreational purposes).
- Data controllers who only process personal information for the maintenance of a public register.
- Data controllers who do not process personal information using automated means.

Data controllers who might fall under one or more of these exemptions can still add themselves to the register voluntarily if they consider it will aid the transparency of their processing.

There have been some recent changes to the notification fees structure that mean the largest data controllers now pay a fee of £500 each year but medium and small organisations still pay only £35 each year. The fees structure and the exemptions from notification favour small businesses and seem to be fair and working well in practice. The Commissioner's view is that the burdens on data controllers should be reduced but this should be achieved by reducing the information that has to be supplied by the majority of those who notify rather than by significantly increasing the numbers who are exempt from notification.

Question 27. Do these current exemptions to notification strike the right balance between reducing burdens and transparent processing?

The Information Commissioner considers that the exemptions from notification and the fees structure strike the right balance between transparency and the financial and administrative burdens on organisations in the UK.

However, the obligation to notify processing is derived from the EU Directive and the Information Commissioner considers that the purposes

[20] A summary is available at: https://www.javelinstrategy.com/brochure-158
[21] Published by Hunton and Williams, available at: http://www.huntonfiles.com/files/webupload/CIPL_Dos_and_Donts_White_Paper.pdf

and system of notification should be reassessed under a future legal framework – in particular as to what details are provided as part of notification. It is clear that notification is implemented differently in Member States under the current EU Directive and that it is used differently by data protection authorities. It is also clear that many organisations view it as a bureaucratic burden that in its current form, with the level and nature of detail required, has few obvious benefits for organisations, individuals or the regulator – although some regulators are funded through notification fees. This form of funding helps a data protection authority achieve independence from government. It is important to the ICO and the Information Commissioner would not want this possibility lost.

A notification system would be more proportionate if there was a requirement for every organisation to simply register their basic contact details. The current obligation to notify processing operations could be replaced by an obligation requiring in principle all organisations to register. However, the content and the method of the registration should be made very simple, via electronic means only. The details supplied could be confined to the data controller's name and address, contact details, and broad description of the purpose of processing operations that the data controller intends to carry out. If an organisation has a data protection officer (DPO) in place, the DPO would be the main contact person in the registration details. The purpose would not be to provide for verification of the processing operations (prior checking), but for data controllers to identify themselves as such and openly take responsibility for this role. The content of the registration should be easily and publicly available, as it is in the UK, again via electronic means. Regulators would benefit from the reduced bureaucracy but they would still be able to contact an organisation in case of complaints or to direct advice or enforcement action.

In some cases notification might include the provision of information about steps an organisation has taken to protect privacy. This second level of notification could be voluntary, except for those data controllers carrying out processing deemed particularly risky or which particularly affects the rights and freedoms of individuals. Criteria would be needed to determine the level of risk of data processing operations that it would be mandatory to notify under this second level of notification.

Under this notification obligation, data controllers would be required to describe the different aspects of their processing (including the nature of data, their retention, security measures and so on), and provide certain information about the steps they have taken to protect privacy, such as privacy impact assessments, binding corporate rules, internal governance procedures and ISO certification. Organisations that would be required to notify under this second level should already have in place some suitable form of internal governance. This approach would allow them to use the information created for their governance procedures as part of notification.

The information included in a second stage notification would be of genuine value to the ICO in carrying out its regulatory functions. Providing regulators with the information outlined above would also have a secondary benefit in requiring organisations that are not already doing so to assess their information governance arrangements in detail and establish what data they hold, what they do with it, and how they comply with the law. Individuals would benefit as they would get a better idea of what a particular organisation is doing with their data and how it is looking after it.

Such an approach would also be relevant to complaints where it could be shown that an organisation did not live up to its stated commitments. It would also help regulators better target organisations and sectors for monitoring or audit, as it would help them to establish where there is the greatest risk for individuals and direct their resources accordingly. For example, they could focus on those organisations with little evidence of compliance and accountability measures, rather than those with clear internal governance procedures, privacy impact assessments and binding corporate rules in place.

The aim is that notification should become a process which is much more useful to the data controller and the regulator, rather than being a purely administrative burden. In addition to the information provided as part of notification, the legal framework should provide for a harmonised EU-wide system for notifying. In particular**,** the legal framework should provide for standard EU-wide templates, both for the basic level registration and for the full notification. This would minimise the effort expended by a data controller that needs to register/notify in more than one member state due to the fact that the format of the documentation required in each member state would be the same or at least very similar.

This could also be a shared platform which would enable data controllers to register or notify the same data processing operations to different data protection authorities at the same time. For example, a data controller would fill in a standard online form and tick boxes to signify the member states in which it wants to notify. Those authorities could then be informed automatically.

Taken together, these measures would significantly reduce the burden of notification while providing genuine benefits to the data controller and national data protection authorities.

Powers and penalties of the Information Commissioner

Question 28. What evidence do you have to suggest the Information Commissioner's powers are adequate to enable him to carry out his duties?

The Information Commissioner is broadly satisfied that the powers available to him enable him to carry out his duties. In particular over the last few years there have been moves to increase both the Commissioner's powers and the resources available to him to deploy those

powers effectively. The Commissioner has a range of powers at his disposal now that include enforcement notices, information notices, the power to audit central Government departments without their consent, powers of entry and inspection and the power to levy monetary penalties of up to £500,000 on data controllers for serious breaches of the data protection principles.

The Information Commissioner considers that there are currently three areas where he needs to have greater powers of enforcement in order to carry out his duties more effectively. These are dealt with in the following questions.

The implementation of the current EU Directive has resulted in many differences in the roles, remits and powers of national data protection authorities. What should the mixture of education, 'policing', complaints handling and policy activity be? Whilst some degree of diversity between national data protection authorities is healthy and perhaps inevitable, the Commissioner recognises that the current situation can be confusing for data controllers that operate internationally – are they dealing with a tough policeman or a helpful educator in any particular country? It would be helpful if a future legal framework could do more to clarify what features and characteristics a modern data protection authority should have. In particular, the Information Commissioner is of the opinion that the role of the national authority as educator must be maintained as an explicit part of any new legislative framework.

There is also a need to be realistic about the functions data protection authorities are expected to carry out, against a backdrop of limited resources and increasing demand for their services. Again, a future framework could do more to help data protection authorities to focus on areas of particular privacy risk, rather than requiring them to 'police' every aspect of the processing of personal information. As explained above, a future framework should encourage data protection authorities to focus more on outcomes, rather than encouraging them to see compliance with the law as an end in itself, even where non-compliance does not put privacy significantly at risk.

If data protection authorities are to deliver useful outcomes, they must have the appropriate tools and resources. A future framework could do more to guarantee data protection authorities' independence, to clarify their role and specify their powers. This is one area where the legal framework would benefit from greater prescription, such as an obligation on governments to consult the data protection authority when laws with a significant impact on information privacy are being introduced.

The Commissioner believes that a future framework could do more to encourage data protection authorities to develop tools to help organisations to adopt good practice, and to help individuals to protect their own personal information and make well-informed privacy choices. Organisations should also be encouraged to 'self-regulate' as far as possible, for example by adopting sectoral codes or applying recognised standards for collecting and handling personal information. The

Commissioner has no doubt that effective self-regulation by organisations (perhaps backed up by some form of accreditation), and self-protection by well informed individuals, are important elements of a modern data protection regime. A future framework should acknowledge and promote this.

With complaints handling, data protection authorities need the freedom to set up procedures to suit their resources and the local conditions. For example, it would be helpful if a future legal framework provided a clear basis for data protection authorities to approve other complaint handling mechanisms, so as to be able to work with other relevant regulators or industry groups who may be able to achieve better or more cost effective results for individuals. The Commissioner has significant doubts as to the sustainability of a state of affairs where data protection authorities are expected to deal with every complaint about every aspect of the processing of personal information. Data protection authorities should be able to be selective, pursuing only those complaints that reveal real potential for damage or distress to the individuals concerned.

Data protection authorities must also be willing to share their responsibilities with others, if this results in better outcomes for individuals. For example, data protection authorities should also be able to support alternative dispute resolution and other forms of redress for individuals. It is clear that in many countries it is not realistic to expect individuals to seek redress through the courts.

A final point is about prior checking in the current EU Directive, known as "preliminary assessment" in section 22 of the DPA. The Information Commissioner notes that this provision has never been commenced in the UK and has doubts about the value of prior checking. If this provision is retained it should be clear that prior checking is not the norm and is confined only to the most risky processing operations.

Question 29. What, if any, further powers do you think the Information Commissioner should have to improve compliance?

It is clear that on some occasions it is not the "data controller" itself that is responsible for data protection breaches – it is an individual who is working for or contracted to the data controller, acting in contravention of the organisation's policies and procedures, or an individual who obtains information from the organisation without their knowledge or consent. This is addressed by Section 55 of the UK DPA.

It is widely evidenced that the greatest threat to information security in organisations is individuals, yet the DPA only provides for a fine for those individuals who knowingly or recklessly obtain or disclose personal data, or procure someone else to do this for them. A fine of up to £5,000 is available in the Magistrates Court, or an unlimited fine is available in the High Court. The Information Commissioner considers that the trade in personal information justifies the possibility of a custodial sentence for the most serious offences. In two reports laid before Parliament, "What Price

Privacy?"[22] and "What Price Privacy Now?"[23], the previous Commissioner laid out the case for custodial sentences for the most serious breaches of Section 55 of the DPA. In response Section 77 of the Criminal Justice and Immigration Act 2008 gave the Secretary of State the power to introduce by order custodial sentences, for unlawful obtaining etc of personal information.

In December 2007 the BNP circulated a membership list to selected party members to be used only for specified party purposes. Following an internal dispute, two BNP members left the party. Both individuals had possession of the circulated list of members. Between 12 and 18 November 2008 the membership list was posted on the internet and was made publicly available without the consent of the BNP. The list contained the names, addresses and contact details of the party members.

On 1 September 2009 one of the ex-members of the BNP appeared at Nottingham Magistrates Court in front of the District Judge. He pleaded guilty to unlawfully disclosing the list, contrary to Section 55 DPA 1998. He was fined £200 and ordered to pay £100 costs. The District Judge commented "the fine was low because the defendant was on benefits" and "it came as a surprise to me, as it will too many members of the party (BNP), that to do something as foolish and as criminally dangerous as you did will only incur a financial penalty".

Since then the ICO has uncovered further cases involving both public and private sector organisations which were detailed in the Information Commissioner's response to the Ministry of Justice's consultation paper on "the knowing or reckless misuse of personal data: introducing custodial sentences"[24]. The then Information Commissioner believed when Section 77 of the Criminal Justice and Immigration Act 2008 was introduced that custodial sentences were needed. The current Information Commissioner considers that the case for the introduction of custodial sentences for section 55 offences is now even more convincing.

A connected concern around the Commissioner's powers is the limitation of his powers to obtain information in connection with his investigations where that information is held by a third party, rather than the data controller. Information notices can only be served on data controllers, and this can unreasonably impede investigations where a third party is believed to hold information which is pertinent to the investigation.
.

[22] Available at http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf
[23] Available at http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico-wppnow-0602.pdf
[24] Available at http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/section_55_response_to_moj_consultation_20091112.pdf

Question 30. Have you had any experience to suggest that the Information Commissioner could have used additional powers to deal with a particular case?

The Information Commissioner has always sought to make the best use of his powers as provided by the current regulatory framework.

The Information Commissioner can in most cases only audit data controllers if they provide their permission. He is currently gathering evidence to show how many data controllers are willing to give this consent when asked and how many refuse. Early indications are that private companies are particularly reluctant to accede to his requests.

A good example of this was when the ICO asked a financial institution in the UK if it could audit their arrangements for outsourcing to a data processor in India. Several requests were made to the financial institution, but they never acceded to the request. The Information Commissioner did not have any direct evidence of non-compliance with the DPA as such, but had sufficient information to indicate that there was a risk of non-compliance that needed to be investigated. There was also a need at the time to provide reassurance to individuals about the protection of their personal data in overseas call centres.

An example of the limitations of the Commissioner's information notice powers is where he is investigating unsolicited marketing calls. It is vital that the name and identity of the caller is made known to the Commissioner, so he has evidence to base any enforcement action. However, this information may only be held by the telecommunications company that carried the call. The Commissioner has no power to compel the disclosure of this information, as the telecommunications provider is not the "data controller" in such cases.

Beyond the issue of his own powers, the Information Commissioner is convinced that any new legislative framework must take a holistic approach to the protection of personal information, allowing the various regulatory bodies and legislative regimes to work together more effectively to protect personal data and prevent gaps in the current regulatory regimes.

The Principles-based Approach

Question 31. Do you have evidence to suggest the current principles-based approach is the right one?

There is no doubt that the current data protection principles are sound and should be maintained. They have generally stood the test of time well and are respected within Europe and beyond. However, what are treated as 'the principles' under UK law extend beyond Article 6 of the EU Directive to include security, transparency and so on. The Information Commissioner favours this approach and hopes that it will be retained in a future legal framework. This highlights the importance of the principles as the backbone of the legislation, although this might be highlighted further

if they were included in the main body of the DPA, rather than appearing as a Schedule to the Act.

The Information Commissioner considers that efforts should be made to make the principles more internationally applicable by bringing about a greater degree of harmonisation with other international instruments, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The international standards adopted at the Madrid international commissioners' conference in November 2009 could play an important role here.

In adding to the principles, the Information Commissioner considers it would be helpful to include elements relating to privacy by design and accountability. With privacy by design, the principles could state that processing of personal data should be done in the least privacy intrusive or most privacy friendly way possible. This could be tied into the current security principle requirement to implement technical measures to protect, not just against security breaches, but against all unlawful forms of processing. It could also be tied in with rules about necessity, relevance and excessiveness of processing. This would give a clear message, especially to those providing and commissioning information technologies, that privacy protection must be a fundamental part of the system design and procurement process.

With accountability, the international standards referenced earlier do contain a separate accountability principle, and it is important that this is accommodated in the data protection framework, although there may be a variety of ways to achieve this.

Question 32. Do you have evidence to suggest that the consent condition is not adequate?

There is confusion about consent under the current legislative framework. This takes the form of confusion between transparency and consent, confusion as to whether consent can be opt out, as well as opt in, and a common misunderstanding that consent is always necessary before processing of personal data can begin. The confusion about consent exists for both data controllers and data subjects.

Articles 10 and 11 of the EU Directive deal with information given to the data subject, commonly referred to as transparency; Article 7 refers to consent. In addition, Article 6 of the Directive says that personal data must be processed fairly and lawfully. There is general acceptance among data protection authorities that fairness has two main elements: transparency and consent. However, the relationship between these two aspects of fairness can be confusing. An emphasis on consent rather than transparency, or vice versa, can give a very different complexion to data protection regimes across Europe, can confuse individuals and cause great practical uncertainty for data controllers. In many cases it is not clear where consent is necessary or where transparency suffices. This can lead to unrealistic presumptions about the degree of control that individuals

should enjoy, perhaps in cases where choice may not be a realistic option or where individuals may neither expect nor want to choose.

This can be a particular issue in justice, home affairs, law enforcement and other public sector contexts. Any future legal framework should be realistic about the extent of choice that individuals can actually have and the degree of choice they actually want. In online contexts it is particularly important, therefore, that browser and website defaults are set in a way that balances functionality and privacy protection appropriately. A requirement for consent can be an important protection for individuals but it should be reserved for situations where an individual genuinely has a free choice as to whether or not to agree to the processing of their personal data.

Whatever form consent takes, any new legislative framework should be clear about what consent actually entails, and whether and when explicit consent is necessary.

Question 33. Should the definition of consent be limited to that in the EU Data Protection Directive i.e. freely given specific and informed?

The Information Commissioner believes that the definition of consent is workable but there needs to be more clarity in any future legislative framework on the nature of consent, when consent is necessary and what would constitute grounds for opt-in and opt-out forms of consent. It is important that the requirement for consent to be freely given, specific and informed is retained. If this provides an unrealistic obstacle to necessary processing of personal data then another basis for legitimising such processing should be available. This does not mean consent necessarily has to be explicit, but it should always be demonstrable.

Question 34. How do you, as a data controller, approach consent?

The Information Commissioner's position on consent is detailed in "The Guide to Data Protection"[25] and is repeated below.

'You will need to examine the circumstances of each case to decide whether consent has been given - and whether it's appropriate. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent. Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as:

"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

[25] Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf

The fact that an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a customer's failure to return a form or respond to a leaflet.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if your organisation intends to continue to hold or use personal data after the relationship with the individual ends, then the consent should cover this. Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, you should recognise that the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which you are collecting or using the information. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given. You should review whether a consent you have been given remains adequate as your organisation's relationship with an individual develops, or as the individual's circumstances change.

Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

The Data Protection Act distinguishes between:

- the nature of the consent required to satisfy the first condition for processing; and
- the nature of the consent required to satisfy the condition for processing sensitive personal data, which must be "explicit".

This suggests that the individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

As explained above, a particular consent may not be adequate to satisfy the condition for processing (especially if the individual might have had no real choice about giving it), and even a valid consent may be withdrawn in some circumstances. For these reasons an organisation should not rely exclusively on consent to legitimise its processing. In our view it is better to concentrate on making sure that you treat individuals fairly rather than on obtaining consent in isolation. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing personal data.'

As a data controller, the Information Commissioner does not seek to rely routinely on consent as there are usually more appropriate conditions for processing, such as the processing being relevant to our functions or it is necessary for the ICO as an employer. On many occasions the ICO would

simply inform individuals about what it intends to do and gives them a chance to object, for example when the ICO has been asked to release details of staff salaries. There are some occasions where the ICO would ask for explicit consent, for example from a complainant when it is necessary to refer their complaint to another regulator in the UK or where contact is made by someone acting on behalf of an individual, such as a solicitor.

Question 35. Do you have evidence to suggest that data subjects do or do not read fair processing notices?

In 2007 the then Prime Minister asked Dr Mark Walport of the Wellcome Trust and Richard Thomas, the then Information Commissioner, to undertake a review of the framework for the use of personal information in the public and private sectors. The Data Sharing Review[26] was published in June 2008 and stated:

"We have seen countless examples of privacy notices that are obscured by their length and language. Privacy notices should be written for public consumption, should be genuinely informative and understandable to their target audience. Privacy notices drafted in anything other than concise, plain and straightforward language are unhelpful, and virtually guarantee they will rarely, if ever, be read. Many data controllers need to improve the way they explain their use of personal information to the general public."

The Data Sharing Review recommended that "fair processing notices" should be made more user friendly, and be written for public consumption. The recommendations also called for fair processing notices to be termed "privacy notices", for clear, simple language to be introduced and for the use of a layered approach to notices. This involves providing a relatively simple initial explanation but one that is backed up by more detail for those who want a more comprehensive explanation. The ICO took these recommendations on board and published its Privacy Notices code of practice[27] on 12 June 2009.
The Information Commissioner considers it important that any future legal framework should be more explicit about the use of tools to provide genuine transparency, such as privacy notices and the publication of privacy impact assessments.

Question 36. Do you have evidence to suggest that the exemptions are fair and working adequately?

There is some confusion around the exemptions, in particular the usefulness of the concept of "non-disclosure provisions" and "subject information provisions", defined in Section 27 of the DPA and used throughout Part IV.

---

[26] Available at: http://www.justice.gov.uk/reviews/datasharing-intro.htm
[27] Available at: http://www.ico.gov.uk/for_organisations/topic_specific_guides/privacy_notices.aspx

A problem the ICO encounters is a lack of understanding of how prohibitions on disclosure that exist outside the DPA interrelate with the provisions and exemptions in the Act. Although Section 27(5) is reasonably clear there can still be difficulty in ensuring that subject access rights are respected where a statutory bar is in place that is not specifically referred to in the DPA or associated regulations.

Another issue the ICO has experienced is where other laws and policies have the effect of undermining the protections provided as part of the DPA, and attempt to go further than the exemptions to the Act allow. A good example of this is how the requirement for local authorities to develop a licensing policy is being implemented. All licensing authorities are required to produce a licensing policy. Many of these licensing policies present the installation of CCTV as a model condition for obtaining a licence to sell alcohol and include provision that CCTV images should be provided to local police services "on request". This wording does not fit in with the provisions of Section 29 of the DPA (which requires a prejudice test) and could be seen as contradicting the UK's obligations to implement the provisions of the European Data Protection Directive. There needs to be an explicit mechanism that ensures that new UK laws and public policies that impact on the processing of personal data are consistent with the UK's obligations under the EU Directive.

Question 37. Do you have evidence to suggest that the exemptions are not sufficient and need to be amended or improved?

Currently the Information Commissioner does not have explicit provision in Part IV of the DPA to withhold personal data in response to a subject access request from an individual where he has received information about that individual in the course of exercising his functions. Whilst the Commissioner and his staff might be committing an offence under Section 59 of the DPA if they disclose that information it is unclear how Section 59 relates to Section 27(5) when applied to personal data held by the Commissioner.

Where this becomes a problem is where an exemption to subject access to particular information is being applied by the data controller but the same exemption cannot be applied by the Commissioner to the information if it has come into his hands in the course of an investigation of the data controller. It cannot be right that an individual might be able to obtain information through a subject access request to the Commissioner that they cannot obtain through a request to the data controller. This needs to be put beyond doubt in the law by an amendment to the exemptions.

With regard to Article 3(2) of the EU Directive, a better definition is needed of what constitutes a 'purely personal or household activity'. Changes in technology and society, such as the growth of social networking sites, mean that there are different interpretations by national data protection authorities of where the limits of personal and household activities lie.

The Commissioner's view is that it is not necessarily the purpose of data protection law to regulate the processing of personal information by one private individual about another private individual, and that a revised Article 3(2) exemption should be included in the new framework. However, where social networking or other sites are being used for non-personal processing, for example, to gather information about a job applicant, or to carry out commercial publication, then the normal rules of data protection must apply. This is not just a question of the limits of where data protection law should apply, but also one of how far the law should go in restricting the fundamental right of freedom of expression.

The fundamental right of freedom of expression is even more relevant to Article 9 of the EU Directive. The increase in the ability of individuals to act as 'journalists', through online publishing, blogging and similar activities, means that this provision is increasingly difficult to apply. Clarification is needed of the balance between processing of personal data and freedom of expression in a world where newspapers and professional journalists have certain obligations as data controllers, but citizen bloggers carrying out the same activities have no obligations or accountability under data protection law. The Commissioner thinks it would be useful to give some thought to whether, or to what extent, data protection law ought to apply to individuals who, in one sense, are engaged in a purely personal activity, yet may have the same potential as a newspaper editor to publish information that could damage other individuals. The Information Commissioner is not suggesting that a future data protection legal framework should necessarily cover individuals' personal activity. However, this is an area that deserves serious consideration, as the demarcation between personal and public activity becomes increasingly blurred.

Another exemption that needs closer examination is the exemption for disclosures required by law. Whilst it is reasonably clear that the reference to a disclosure required under an enactment means a disclosure required under UK statutory provisions, it is unclear what is meant by a disclosure required by "any rule of law". Is this a UK law, a rule of law of an EEA Member State or any rule of law that exists anywhere in the world however far reaching that might be?

International Transfers

Question 38. What is your experience of using model contract clauses with third countries?

The experience of the regulator is that while the model contract clauses are useful, they have limited applicability and there is much confusion about their use. The Commissioner regularly receives questions about whether model contract clauses can be altered and the transfers they govern still be considered to be subject to "adequate" protection. Many legal advisers seem to view model contract clauses almost as a template from which they can derive their own version of the clauses without realising that the model clauses are the only ones that would automatically be considered to provide adequate protection.

Question 39. Do you have evidence to suggest that the current arrangements for transferring data internationally are effective or ineffective?

The current system for determining whether a third country has an adequate level of data protection is slow and cumbersome, and only a few countries have to date achieved an adequacy finding from the EU Commission. This system may still be part of the solution in the future legal framework, but it needs to be a quicker and simpler process. The future legal framework should also reaffirm the position that the test is adequacy, not equivalence. However, EU Commission findings of adequacy should not be the only option; there need to be more flexible solutions for recognising the adequacy of organisations or sectors in non-adequate countries. For example, recognising those signed up to recognised industry codes of practice, or approving self-regulatory systems. There is also a link here to the points made on accountability, with the possibility that properly accountable organisations in third countries could be deemed adequate for the transfer of personal data.

To the extent that the current provisions of Article 26(2) of the Directive, which relates to authorisations of transfers where the controller determines there is adequacy, and which references contractual clauses are retained, the Commissioner suggests adding the option for the Article 29 Working Party to approve other mechanisms. The Commissioner favours a system that approves methods of transfers, not the individual transfers. Any approval of a method of transfer (such as contractual clauses, BCR) should be underpinned by a legally established system of mutual recognition.