

# Data Protection Strategy Consultation Draft



# Contents

Our vision and our purpose	3	Partnerships	15
This strategy	4	Our expectations of others	17
Our approach	5	Our international role	19
Data protection risk	7	Where does this take us?	20
Setting priorities	9	Annex - Data protection functions	22
How we intervene	13		

## Basic information regarding this consultation

**To:** Anyone interested in how the information Commissioner's office goes about minimising data protection risk, the long term effectiveness of our office and the bringing about of good practice.

**Duration:** From 02 July 2007 to 28 September 2007

**How to respond:** **In writing:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow SK9 5AF care of our Customer Support Team.

**By email:** [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk) marking the subject heading 'Data protection strategy consultation'

## Our vision and our purpose



Data protection lives in the real world. It is all about people and what happens to information about them. The collection and use of personal information is essential to the functioning of our modern society. Our vision is of a society where respect for personal information is guaranteed. A society where organisations inspire trust by meeting reasonable expectations of integrity, security and fairness in the collection and use of personal information. A society where individuals understand how their information is used, are aware of their rights and are confident in using them.

Our data protection purpose is to make this vision a reality. At its heart is ensuring, in a responsible and measured way, that the rights and obligations set out in the Data Protection Act 1998, the Privacy and Electronic Communications Regulations 2003 and related legislation are respected. This means that we are primarily concerned with regulating the processing of personal data by the state, by businesses and by other organisations and not with processing by individuals in their purely personal capacity.

However we are not seeking compliance with the law as an end in itself. Making our vision a reality means minimising data protection risk for individuals and society. The law is the main tool we have at our disposal to achieve this, but we go further and promote good practice. Good practice may go beyond simply meeting the requirements of UK law but will always be consistent with the law as well as with the EU Data Protection Directive (95/46/EC) and ultimately with the right to respect for private life enshrined in Article 8 of the European Convention on Human Rights.

## This strategy

This data protection strategy sets out how we go about minimising data protection risk. It is concerned with ensuring our maximum long term effectiveness in bringing about good practice. This strategy is aimed at our major stakeholders and spells out the basis on which we select:

- **the issues on which to engage;**
- **the outcomes we seek; and**
- **the approach taken to engagement.**

This strategy will serve as a reference point for our staff, for all their data protection work. Separate papers deal with the application of this strategy in specific areas such as case handling and the use of our formal powers to take regulatory action.

## Our approach



Being a strategic regulator means that, in so far as we have a choice, we have to be selective with our interventions. We will therefore apply our limited resources in ways that deliver the maximum return in terms of a sustained reduction in data protection risk. That is the risk of harm through improper use of personal information.

There are priorities we have to set. We need to focus most attention on situations where there is a real likelihood of serious harm. We also need to focus on situations where our intervention is most likely to make a long term as well as a short term difference. When we intervene we must do so in a way that gives us the best possible return and remember that we will often be at our most effective when working closely with others. We are entitled to have legitimate expectations of those who are in a position to influence data protection risk. Our effectiveness depends on them seeking and welcoming our reasonable interventions. Furthermore we have an important international role. Data protection in the UK is increasingly influenced by events worldwide.

Our risk-based approach is in line with good regulatory practice. It does not mean that we seek to remove all data protection risk. We do what we can to moderate the most serious risks and protect those who are most vulnerable to improper use of their information. But we will not try to take away freedom of choice and will remember that individuals themselves ought to be best placed to make decisions about their own interests. Part of our job is to equip individuals with the knowledge and tools to enable

them to make their own well-informed decisions about the use and disclosure of their personal information.

Being a strategic regulator also means extending our approach beyond simply improving (through guidance, persuasion and regulatory action) the behaviour of organisations that handle personal information. We also have a legitimate role in influencing the market or political environment in which they operate. Thus we will seek to have long term influence over government and the legislature at Westminster and in the devolved administrations as well as over representative bodies and other stakeholders, to ensure privacy friendly outcomes.

We will also seek to influence the legal framework that governs our own work to ensure that data protection requirements are simple, meaningful and proportionate and that we have the flexibility and tools to regulate effectively.

Building public confidence in data protection is key in our approach. We protect people, not just information. This means we need to engage with the public and explain what we do in a way that they can easily understand and relate to. One of our three ongoing priorities is;

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

This commitment is at the heart of how we approach our job as data protection regulator and will inform all our data protection tasks including complaints handling and the provision of advice.

## Data protection risk



The outcome we are seeking is a minimisation of data protection risk – the risk of harm through improper use of personal information. To set our priorities and provide a reference point for our approach to our regulatory activities we need to be clear what we mean by “harm”.

The principal risk which our activities must address is the risk that individuals will suffer harm because personal information about them is:

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

Such individual harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example the loss of a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of financial circumstances. Sometimes harm might still be real even if it is intangible,

for example the fear of identity theft that comes from knowing that the security of your financial information has been compromised.

There is also harm which goes beyond the immediate impact on individuals. The harm arising from improper use of personal information may – at least initially – be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. This societal harm might for example arise through the development of a surveillance society.

Societal harm can have multiple causes but improper use of personal information could be a significant factor in:

- **excessive intrusion into private life which is widely seen as unacceptable;**
- **loss of personal autonomy or dignity;**
- **arbitrary decision-making about individuals, or their stigmatisation or exclusion;**
- **the growth of excessive organisational power;**
- **a climate of fear, suspicion or lack of trust.**

## Setting priorities



We cannot address all areas of data protection risk equally, nor should we attempt to do so. We are spending public money, generated through the notification fee, and must achieve value for money. We are also imposing burdens on businesses and must ensure that the costs of compliance are in proportion to data protection risk. Thus we will set priorities, target our actions where we can and take a measured approach in the lines we take. We will be open about our priorities so that our stakeholders know where they stand.

Our priorities will be influenced by both the seriousness and likelihood of harm and by the extent to which we can make a difference.

### How serious and how likely?

We will make judgements about the seriousness of the risks of individual and societal harm. We will also make judgements about how likely it is that the risk will materialise. We will give priority to tackling situations where there is a **real likelihood** of **serious harm** to individuals or society.

The necessary judgements especially about seriousness are not always easy. Loss of privacy can qualify as a harm in its own right, but there are difficult issues of objectivity and subjectivity. Some individuals value their privacy more than others. Our approach will be as objective as possible. It is cast in the following terms:

- We must be well-informed, learning from our own experience with enquiries, complaints and stakeholder contact as well as from research findings, regular horizon-scanning, and political and market intelligence.
- We will rely as far as possible on evidence about what actually matters to those we are seeking to protect and how likely it is to occur.
- The harm we seek to prevent must always be genuine and be capable of explanation.
- We will reflect the reasonable expectations of individuals and society.

In judging the seriousness of harm we will look beyond the obvious impact on those who submit complaints to us. We will take account of factors such as;

- the number of individuals actually or potentially affected;
- whether these individuals are particularly vulnerable;
- the long term as well as the short-term impact on those affected;
- whether the harm is a one-off or part of a pattern or trend;
- harm that arises indirectly because public confidence in data protection is damaged.

## Can we make a difference?

Judgements are also required about where we can realistically make a difference in reducing the likelihood of harm. We will ask ourselves if our intervention is likely to produce a worthwhile return on the effort we might invest. We will also ask ourselves whether our intervention is key to a successful outcome or whether we can rely

on the efforts of others. We will take into account the reasonable expectations of our stakeholders as to where and when we should engage. In doing so we will ask ourselves how closely the issue is related to our core business of ensuring respect for the rights and obligations set out in the law. As before we will ensure that as far as possible our judgements are evidence based. Questions we will ask ourselves include:

- Is there a need for us to display leadership?
- Is there a genuine data protection issue or is data protection merely an aspect of a bigger problem?
- Can we expect to make a real, long term difference for example by stopping the excessive collection of personal information?
- Are governmental initiatives, new UK or international policies or new legislation in prospect that we might influence?
- Are there technological advances or commercial developments that we might influence?
- Are there other opportunities, for example media interest, that we might take advantage of?
- Are there gaps or inconsistencies in our approach, with pressure for our engagement?
- Are the data protection risks being addressed already, for example by, market forces or the actions of other regulators?

We will set priorities but we do not have complete freedom as to how we allocate our resources. We are obliged to consider complaints that are brought to our attention

and we must respond positively to those who need our advice. In doing so we must maintain proper standards of customer service. Nevertheless we will do what we can to direct our resources towards situations where there is, or is a likelihood of, real harm and where our intervention can limit this.

One consequence of our approach is the likelihood that we will need to devote proportionately more of our policy work to developments in the public sector than to developments in the private sector. This is a recognition of where the most serious data protection risks can arise.

CONSULTATION DRAFT

## How we intervene



We have limited resources and need to use them as efficiently as possible. Whilst dealing with real problems faced by individuals our complaints and advice services will inevitably remain reactive. However we will seek to be influential working where we can to head off data protection risk before it materialises rather than responding to problems as they arise. In particular we will:

- Work on the basis that prevention is better than cure.
- Take steps to ensure that data protection aims are given due weight in the early stages of the development of policy and legislation, rather than merely addressing the consequences when it may be too late to achieve anything.
- Provide information, advice and other help to organisations seeking to achieve high standards rather than penalising them when they get it wrong.
- Place particular emphasis on privacy-friendly approaches, minimising the collection of personal information, ensuring its accuracy and keeping it secure as well as making it easier for individuals to access their information and exercise their rights.
- Seek sustainable, long term reductions in data protection risk rather than just short term fixes.

- Equip individuals to exert pressure themselves by asking the right questions and making their own choices.
- Recognise the role of reputation, consumer pressure and market forces in delivering good practice particularly with reputable private sector businesses.
- Give due weight to the views of those with expert knowledge of relevant business practices.
- Work in concert with other regulators clarifying our respective roles, taking the lead where it is necessary for us to do so but leaving it to others where they are achieving desired outcomes.
- Support regulatory forces by providing incentives for good practice such as accreditation and awards.
- Recognise that our interventions can involve burdens and costs and, where they do, ensure that our approach is balanced and proportionate.
- Ensure that in all our interventions we reflect issues of genuine public concern and that we command public confidence.

We recognise the importance of being imaginative about how we intervene. We are open to new ways of working and new forms of engagement with our stakeholders.

## Partnerships



We have to work on data protection with other stakeholders, capitalising on their experience, powers, reputation and influence to achieve our purpose. In particular we need to develop our contacts and work with:

- **other statutory regulators:** We are a “horizontal regulator” covering data protection across all sectors. Others are “vertical regulators” covering all activities within a particular sector. There is obvious overlap. Vertical regulators have a key role in helping us develop good data protection practice in the sectors they cover;
- **commercial and self-regulatory bodies:** There is a strong measure of self-interest in organisations behaving well in their dealings with members of the public. Data protection is an element of good business practice. We can tap into self-regulatory initiatives, to ensure they give due weight to good data protection practice;
- **the legislature:** The Westminster and devolved legislatures have the tasks of debating and passing legislation and scrutinising the work of government. They are uniquely placed to promote respect for the privacy of personal information and to identify shortcomings;
- **the media:** We need to get across clear and consistent messages about the purpose and benefits of data protection. This is an essential ingredient of the public confidence on which we rely. We need to work with the media to deliver these messages;

- **data protection and privacy officers:** In house data protection or privacy officers have a key role in influencing the behaviour of organisations They can help us better understand risk, identify where we can make a difference and ensure that personal information is properly protected.
- **civil society and consumer organisations:** We rely on consumer and related organisations to deliver clear and consistent messages to the public on data protection. We need them to tell us what the public, or sections of the public, want and expect from us.

Above all we see ourselves as working with those whose rights and liberty we are seeking to protect and enhance. We have a role in educating the public and raising their awareness and competencies but we must understand and respond to their interests and concerns.

## Our expectations of others



We have to improve the ways in which we gather and use intelligence and be alert to developments with data protection implications. Nevertheless we still need our stakeholders to tell us, at an early stage, when they embark on developments that carry a significant data protection risk. They should not be afraid to do so. Our role is to help them achieve their objectives in a privacy friendly way not to act as a barrier to sensible progress.

On the other hand we expect our stakeholders to make use of and apply the guidance we produce. It is not good use of our time to respond individually to requests for advice where the necessary advice is available in published form. If our published advice does not meet the needs of our stakeholders we would like them to provide feedback to us. It is also helpful if our stakeholders bring us their thoughts on minimising data protection risk, based on their knowledge of their own fields of business.

We place particular value on developing our relationship with the legislature. We expect the Westminster and devolved administrations to give due prominence to the reduction of data protection risk as a desirable outcome of the legislative process. We want them to use us as a trusted and respected adviser and we expect to be invited to contribute where our involvement can assist this process.

We expect the Government to honour its commitment to pursue the enhancement of privacy alongside its objective of making better use of personal data to deliver improved public services. It is particularly important that we are involved not only at the early

stages of policy development which might impact on data protection risk but also at the early stages of development of systems where the processing of personal data is a significant element. We will seek formal commitments from government departments in Whitehall and the devolved administrations to engage with us at those points where we ought to be involved.

We value our contact with civil society and non governmental organisations. They have an important role in drawing our attention to current and potential data protection risk and reflecting the concerns of individuals. We will listen to their claims provided they are supported by evidence and argument.

CONSULTATION DRAFT

## Our international role



We have an important and developing international role. Not only do we have specific duties related to international cooperation and supervision but we operate in an era of ever-increasing globalisation. Data protection risk is no respecter of international borders. If we are to be effective in reducing risk in the UK we have to be willing to engage with those who determine that risk whether they are based in the UK or elsewhere. This will include EU bodies, inter-governmental organisations, international trade associations and multi-national businesses.

Furthermore if we are to strengthen public confidence in data protection by taking a practical down to earth approach we cannot look at the UK in isolation. We must work with other authorities, particularly those inside the European Union, to improve the image, relevance and effectiveness of data protection worldwide.

Ultimately, simplification for international organisations means one set of data protection standards that are applicable throughout the world. It will not be easy but we have a key role in helping to deliver these. Our experience and size means that we are expected to play a leading part in international data protection affairs. We welcome this but we must bring the same risk based approach to our international data protection work as we do to our domestic activities. This means that we must be selective in taking up the opportunities available at international level and use them to best long term effect.

## Where does this take us?

This strategy serves as a reference point for all our data protection work. In so far as we have the freedom to do so, it is particularly valuable in helping us choose the issues on which to engage. Both the issues and their relative priorities will change over time. Nevertheless it is possible to identify some themes which, for the foreseeable future, are likely to remain high on our agenda. These are:

- **The unlawful trade in confidential personal information:** As well as prosecuting those involved we will use our influence to help bring the unlawful trade to an end. We will work to raise awareness and standards and educate individuals about how they can best protect their own information.
- **The emergence of a surveillance society:** We will continue to stimulate public debate on the impact and desirability of increased surveillance both for individuals and society. We will also seek to mitigate the negative effects of surveillance by promoting privacy friendly approaches, influencing stakeholders, developing relevant tools and increasing the confidence of individuals in exercising their data protection rights.
- **Increased information sharing:** We will work hard to promote good practice when personal information is shared, concentrating on the risks inappropriate information sharing can pose for individuals. We will expect organisations to give due weight to data protection considerations paying particular attention to sharing that crosses sectoral boundaries. We will develop guidance and privacy friendly tools and approaches. Where obligations are ignored we will consider the use of our formal enforcement powers.

- **Law enforcement activity:** Increased collection, exchange and retention of personal information by law enforcement agencies bring clear risks for individuals. We will use our influence with government and the legislature and engage with law enforcement agencies to ensure that any impact on privacy is justified by law enforcement gains and that personal information is handled responsibly. We will also seek to influence EU developments so that a data protection framework for law enforcement is put in place that is both simple and effective.
- **Security of personal information:** Ensuring the security of personal information is a key data protection objective. Individuals expect the Data Protection Act to protect the security of their information. At the same time security is increasingly at risk. Ever growing collections of personal data, more remote access and the prevalence of crime such as identity theft all create vulnerabilities. We will promote the importance of appropriate security, use our regulatory powers where responsibilities are neglected and help individuals to protect their own information.
- **Effective data protection supervision:** We will work hard to simplify data protection, build our own effectiveness as a regulator and promote public confidence in data protection in the UK. We will ensure the effectiveness of our casework and advice services, recognising that these are our key points of contact with a concerned public and that we are committed to addressing matters of genuine public concern. We will also work with other data protection authorities particularly within the EU, to improve the effectiveness of data protection worldwide. We will promote cross border and even global solutions to data protection risk where these are likely to prove the most effective means of making a long term difference.

## Data protection functions of the Information Commissioner's Office

This annex explains briefly what the Data Protection Strategy means in practice for some of the data protection functions of the Information Commissioner's Office.

### Educating and influencing

- **Individual awareness:** We have a major role in giving advice and more generally raising the awareness of individuals about how their info is used and the rights they have. An aware and questioning population is a key partner in data protection regulation.
- **Guidance:** We will continue our programme of clear and unequivocal guidance to organisations and to individuals but ensure that we establish priorities based on data protection risk. We must find out if and how our guidance is being used and whether there is more we can do to improve its relevance and accessibility.
- **Promoting privacy protection:** We will actively promote privacy protection as an aim in developments that rely on the processing of personal information. We will also promote an understanding of the broad principles of data protection as an aid to good decision making within organisations.

- **Influencing the legislature:** We have a legitimate role in influencing governments and the legislature to deliver data protection friendly outcomes. We do not see our role as one of campaigning or of challenging the will of the legislature. Rather we should be a critical but constructive friend seeking to ensure that the position of individuals has been fully taken into account.
- **Technology:** We will watch how technology is developing, spot areas of data protection risk and seek to influence further developments and their application to ensure data protection friendly outcomes.
- **Data protection laws:** We are concerned to ensure that the data protection framework that we apply is simple, targeted and proportionate. Whilst supporting the broad, principle based approach in the current Data Protection Act we will use suitable opportunities to press for improvements in data protection and related laws at European and at national level.

## Resolving problems

- **Complaints:** We must consider complaints that we receive and provide proper standards of customer service but we have choices as to how far we investigate and use our enforcement powers. These choices will be based on our assessment of data protection risk. We will not act merely to solve problems for individual complainants but will concentrate on identifying and addressing significant non compliance. We also need to extract information from the complaints we receive so that we better understand public concerns and the impact of our actions.
- **Advice:** We are committed to giving organisations advice when they need help with compliance. They may contact us without fear of sanction. The investment we put into responding will be dependent on the risk involved.

## Enforcement

- **Regulatory action:** We will apply a risk based approach to the use of formal regulatory action, including prosecution, enforcement notices, 'stop now' orders and audit. This is the subject of our separate Regulatory Action Strategy which sets out clearly what those who might be subject to formal action can expect of us.
- **Notification:** We will continue to ensure that the burden placed on organisations by the notification requirement is kept to a minimum and is proportionate to its purpose. In pursuing cases of non notification we will be guided both by data protection risk and by the need to ensure consistent application of the law.
- **Tools and penalties:** We will actively seek changes to the law that are required to equip us with the tools and penalties that we need for our enforcement function.

If you would like to contact us please call 08456 306060, or 01625 545745 if you would prefer to call a national rate number.

e: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)

w: [ico.gov.uk](http://ico.gov.uk)



June 2007

Information Commissioner's Office  
Wycliffe House, Water Lane  
Wilmslow, Cheshire SK9 5AF

