

Title: Data Protection Act 1998 Lead department or agency: Ministry of Justice (MoJ) Other departments or agencies: Information Commissioner's Office (ICO)	
	IA No: MoJ003
	Date: 26/01/2011
	Stage: Post Implementation Review
	Source of intervention: EU
	Type of measure: Primary legislation
	Contact for enquiries: ollie.simpson@justice.gsi.gov.uk

Summary: Intervention and Options

What was the problem under consideration? Why was government intervention necessary?

The Data Protection Act 1998 (DPA) was required to transpose into UK law the 1995 EU Data Protection Directive 95/46/EC ("the Directive"). In turn, the Directive was needed to establish coherent minimum standards amongst EU Member States, the lack of which had acted as a barrier to the free flow of personal data across the EU. Before this, and in response to an increase in the use of computerised records, standards which would protect personal data were enshrined in the 1981 Council of Europe Convention on Data Protection (Convention 108). The UK introduced the Data Protection Act 1984, which came into force in 1987 and, among other things, provided individuals with certain rights with respect to their personal data. The 1998 DPA revised and replaced the provisions of the 1984 Act when it was commenced in 2000.

What were the policy objectives and the intended effects?

The aims of the Directive were to establish minimum data protection standards throughout the EU; to protect individuals' rights and freedoms, and in particular their right to data protection safeguards; and to facilitate the free flow of personal data within the EU in the interests of improving the operation of the single market. The 1998 DPA was enacted to give effect to the Directive, whilst maintaining the rights for individuals and responsibilities of organisations in relation to the processing of personal data set out in previous legislation (namely, the Data Protection Act 1984 which the 1998 DPA replaced). This was intended to result in organisations improving their information management processes, giving individuals increased confidence that their data are being appropriately handled.

How have the policy objectives been achieved? Please highlight any unintended consequences.

In broad terms, the DPA is working as intended, with most challenges only arising in more limited or technical areas. The DPA has provided the UK with standards which the UK Government believes are in line with European data protection law. However, it is apparent there are still occasions when the DPA is not understood or applied correctly. This means that, in certain areas, the processing of personal data may still be open to abuse or misuse. There have also been examples of organisations citing the DPA incorrectly when deciding not to release information. This has led to the creation of unnecessary barriers to the processing of personal data (for example, in the field of health and social care) which were not intended by the legislation. There is also evidence that some organisations, especially (but not exclusively) in the public sector, are responding to high volumes of subject access requests in the context of employment disputes and litigation, resulting in considerable administrative burdens.

What was the original commitment date to review this policy?

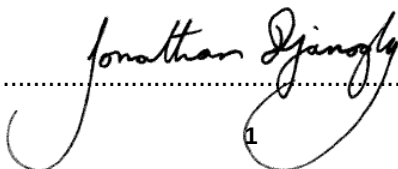
None

If you did not meet the original commitment date to review this policy please explain why.

N/A

Ministerial Sign-off For Post Implementation Review Impact Assessments:

I have read the IA and I am satisfied that it represents a fair and proportionate assessment of the impact of the policy.

Signed by the responsible Minister:  Date: 26 January 2011.....

Summary: Analysis and Evidence

Policy Option 1

Description:

Data Protection Act 1998

Description: Data Protection	PV Base Year N/A	Time Period Years N/A	Net Benefit (Present Value (PV)) (£m)		
			Low: Optional	High: Optional	Best Estimate: N/Q

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	Optional		Optional	Optional
High	Optional		Optional	Optional
Best Estimate	N/Q		£53m	N/Q

Description and scale of key monetised costs by 'main affected groups'

The monetised costs have been borne by data controllers (broadly, any organisation which decides how and why personal data is to be processed) in: providing information to individuals (c£50m); notifying the Information Commissioner of data processing activities (c£3m); seeking expert information from other parties (negligible) (all estimated annual costs). There are also justice system costs borne by the ICO from enforcing the DPA (£1m). However, some respondents to the MoJ's Call for Evidence believed the figures outlined above underestimated the true costs and burdens of compliance with the DPA.

Other key non-monetised costs by 'main affected groups'

Further costs have involved extra staff hired to enforce compliance with the DPA, with related training cost. There have been costs for those organisations that have been served penalties under the DPA and a small impact on the courts and legal aid budget. Some organisations will have invested in software to protect the personal data they hold from misuse or theft. Incorrect application of the DPA may also have stopped agencies from sharing information with wider adverse impacts on crime and possibly health. The DPA may also have an impact on UK firms' ability to enter markets where data protection law is less stringent.

BENEFITS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	Optional		£3m	Optional
High	Optional		£16m	Optional
Best Estimate	N/Q		£9m	N/Q

Description and scale of key monetised benefits by 'main affected groups'

Data controllers may have experienced benefits in terms of avoiding data breaches because of the protections, standards and safeguards that the DPA provides. Whilst it is impossible to establish with accuracy how many major breaches have been avoided and their potential costs, we assume potential savings of up to around £16m per year, with a more likely scenario of around £9m, based on the cost of a data breach calculated by PwC (see page 8). The consolidated fund also benefit from the criminal fines received as a result of DPA related prosecutions by the ICO (negligible).

Other key non-monetised benefits by 'main affected groups'

Businesses have been assisted by the DPA in that it may encourage consumers to (for example) order goods online or join loyalty schemes, confident that their personal data is being held securely. There will have been increased public confidence in the data protection regime. With the DPA's standards in place, organisations in other countries will have had increased confidence to trade and do business with UK companies, Individuals' personal data has been protected by law, with rights of redress when it is misused.

Key assumptions/sensitivities/risks

Discount rate (%)

N/A

We assume that full compliance with the DPA has resulted in fewer data breaches occurring and that the cost of a breach is broadly that set out by PwC in a recent report (up to around £700,000). We also assume that other PwC figures from 2005 represent accurately the admin burdens placed on data controllers by the DPA. The correspondence received by the Department relied upon represents only a limited picture of how the DPA is working for most citizens. We assume that data controllers would not have provided sufficient protections without the DPA, both to secure people's rights and to harmonise standards of data protection across the EU. However, given the scarcity of information on costs and benefits, there is a significant risk that the picture we have is inaccurate.

Impact on admin burden (AB) (£m):			Impact on policy cost savings (£m):	In scope
New AB: £5m	AB savings: 0	Net: £5m	Policy cost savings: N/Q	No

Enforcement, Implementation and Wider Impacts

What is the geographic coverage of the policy/option?			United Kingdom		
From what date was the policy implemented?			01/03/2000		
Which organisation(s) enforce(s) the policy?			ICO/CPS/HMCS/Tribunals		
What is the annual change in enforcement cost (£m)?			£1m		
Does enforcement comply with Hampton principles?			Yes		
Does implementation go beyond minimum EU requirements?			Yes		
What is the CO ₂ equivalent change in greenhouse gas emissions? (Million tonnes CO ₂ equivalent)			Traded: N/Q		Non-traded: N/Q
Does the proposal have an impact on competition?			Yes		
What proportion (%) of Total PV costs/benefits is directly attributable to primary legislation, if applicable?			Costs: 20%		Benefits: N/Q
Annual cost (£m) per organisation (excl. Transition) (Constant Price)	Micro NQ	< 20 NQ	Small NQ	Medium NQ	Large NQ
Are any of these organisations exempt?	No	No	No	No	No

Specific Impact Tests: Checklist

Set out in the table below where information on any SITs undertaken as part of the analysis of the policy options can be found in the evidence base. For guidance on how to complete each test, double-click on the link for the guidance provided by the relevant department.

Please note this checklist is not intended to list each and every statutory consideration that departments should take into account when deciding which policy option to follow. It is the responsibility of departments to make sure that their duties are complied with.

Does your policy option/proposal have an impact on...?	Impact	Page ref within IA
Statutory equality duties ¹ Statutory Equality Duties Impact Test guidance	No	15
Economic impacts		
Competition Competition Assessment Impact Test guidance	Yes	15
Small firms Small Firms Impact Test guidance	Yes	15
Environmental impacts		
Greenhouse gas assessment Greenhouse Gas Assessment Impact Test guidance	No	16
Wider environmental issues Wider Environmental Issues Impact Test guidance	No	16
Social impacts		
Health and well-being Health and Well-being Impact Test guidance	No	16
Human rights Human Rights Impact Test guidance	Yes	16
Justice system Justice Impact Test guidance	Yes	17
Rural proofing Rural Proofing Impact Test guidance	No	17
Sustainable development Sustainable Development Impact Test guidance	No	18

¹ Race, disability and gender Impact assessments are statutory requirements for relevant policies. Equality statutory requirements will be expanded 2011, once the Equality Bill comes into force. Statutory equality duties part of the Equality Bill apply to GB only. The Toolkit provides advice on statutory equality duties for public authorities with a remit in Northern Ireland.

Evidence Base (for summary sheets) – Notes

Use this space to set out the relevant references, evidence, analysis and detailed narrative from which you have generated your policy options or proposal. Please fill in **References** section.

References

Include the links to relevant legislation and publications, such as public impact assessment of earlier stages (e.g. Consultation, Final, Enactment).

No.	Legislation or publication
1	Data Protection Act 1998
2	Regulatory Impact Assessment of Directive 95/46/EC (December 1997)
3	Administrative burdens data (Price Waterhouse Coopers, 2005) www.abcalculator.bis.gov.uk
4	Information Commissioner's Office Personal Information Survey (conducted by ICM Research) (2008)
5	Information Rights Tracker Survey (conducted by the British Market Research Bureau) (January 2010)
6	Data Protection in the European Union – Data Controllers' Perceptions (Flash Eurobarometer Series 226 – February 2008)
7	Call for Evidence on the Data Protection Legislative Framework and Provisional Post Implementation Review of the Data Protection Act 1998 (July 2010)

Evidence Base (for summary sheets)

Background

Problem under consideration

The period between the early 1980s and the mid-1990s saw ways of processing personal data quickly and efficiently becoming more common, and on a larger scale. The dangers posed to safeguarding personal data (for example, through loss, destruction, accidental or malicious disclosure, or inaccuracy) remained the same as those addressed by the 1981 Council of Europe Convention on Data Protection (108) and the Data Protection Act 1984, but it could be argued that the risk of those dangers had increased.

At the same time, EU Member States experienced difficulty in transferring data across intra-EU borders, due to the differing rules governing data processing in different countries. Individuals, businesses and government bodies in one Member State could not have confidence that the same protections would apply to personal data if it crossed a border. A draft Data Protection Directive was therefore introduced in 1990 to help address this problem, and this was eventually adopted on 24 October 1995 as the Data Protection Directive 95/46/EC ("the Directive"). The Directive had to be implemented by Member States by 24 October 1998.

Rationale for intervention

The immediate need to intervene was to transpose the Directive into UK law and thereby avoid infraction proceedings. The Directive made provision for individuals to have rights of access to manual records about themselves, which were not covered by the 1984 Act, so additional legislation was required to implement these. The Directive also provided for increased rights to compensation and redress in the courts. Additionally, various parts of the 1984 Act went further than the requirements of the Directive in safeguarding personal data and it was felt that these needed to remain in force. In this way, the protection of personal data for individuals in the UK would be assured. Finally, full transposition of the Directive into UK law would provide the minimum standards needed to allow personal data to be shared across borders, creating greater potential for the UK to trade and co-operate with other EU Member States.

Policy objective

The policy objective for the UK was to implement the Directive fully, ensuring appropriate protection of personal data. The DPA's objectives therefore mirror those of the Directive, namely:

- to establish minimum standards of data protection throughout the EU;
- to protect individuals' rights, including their right to data protection safeguards; and
- to facilitate the exchange of personal data between Member States, thereby improving the operation of the single market.

The Government's stated aim at the time was to ensure the required level of protection for individuals without putting undue burdens onto data controllers (i.e. those organisations and people who determine the purposes and manner in which personal data is processed) additional to those contained in the 1984 Act. However, this Impact Assessment (IA) considers the burdens and benefits of the DPA as a whole, not just where they differ from the previous legislation.

Groups affected

The DPA has an impact on anyone in the UK who processes personal data. This includes businesses of all sizes, government departments and agencies, and charities. The DPA provides exemptions from some of its requirements under certain circumstances (for example, where national security is involved). Personal data processed only for the purposes of an individual's personal, family or household affairs are largely exempt from the DPA's requirements.

Individuals have also been affected by the DPA by having their personal data protected by the law, with recourse either to the Information Commissioner's Office (ICO) or through the courts when their data is (for example) lost, or processed unfairly. We do not know the extent to which individuals and companies would have experienced these costs and benefits without the DPA (for example, companies may have offered subject access to their customers as a matter of good customer service).

Scope

This Post Implementation Review IA is necessarily conducted at a high level and a full evaluation of the DPA is difficult, given the lack of a pre-established framework to monitor costs, the quality of evidence available, and the resources available to undertake research. This IA is therefore based on preliminary desk research, consideration of previous research in this area and responses to the Government's 2010 Call for Evidence on the Data Protection Legislative Framework, which included some comments on the provisional Post Implementation Review published in July 2010. It is being published alongside a Government Response to the Call for Evidence and is prepared ahead of negotiations on a new European data protection instrument, which are expected to begin in mid-2011.

The situation with regard to data protection cannot be compared with that experienced in the UK before 1984 (when there was no specific data protection legislation), because smaller amounts of personal data were processed at that time in less technologically advanced ways. Comparisons with countries that have no data protection law raise similar difficulties. It is possible that much of the current practice and culture surrounding the security of personal data may well have arisen, independently of whether legislation was in place or not, as matter of good practice among Government departments, businesses and charities.

Costs and Benefits

Base case

The "base case" for this IA is a situation where there is no data protection legislation in place. The Data Protection Act 1984 imposed costs on data controllers and brought benefits to organisations and individuals in the same areas as the current DPA, although, importantly, it did not apply to manual paper files. However, in considering the impact of current data protection legislation, we recognise that most interested parties (including data controllers and members of the public) will look at what costs and benefits are provided for by the legislation currently in place, and will not generally consider how the current Act differs from previous, repealed legislation. We have therefore chosen not to make our base case the situation where the 1984 Act is still in force, but rather the situation where there is no data protection legislation in force along the lines of the Data Protection Act 1984 and the DPA. As such this PIR assesses the impact of having a data protection framework, rather than the impacts of the 1998 act per se.

The information being used

In 2005 Price Waterhouse Coopers (PwC) carried out research for the Government assessing the administrative burdens of various pieces of regulation. These are the costs resulting from information obligations imposed on an organisation, where the organisation would not choose to undertake the administrative activity in the absence of the legislation. Included in the PwC research was the DPA and associated items of secondary legislation. These figures, available through the Department for Business, Innovation and Skills' Admin Burdens Calculator, form the core of our provisional assessment of the admin burdens imposed by the DPA (see https://www.abcalculator.bis.gov.uk/login_register.php). It should be noted that these figures are subject to a large degree of uncertainty.

In addition to the PwC figures, this IA takes into account the Flash Barometer 226 "Data Protection perceptions among data controllers among enterprises in the Member States" telephone survey conducted on behalf of the European Commission. The survey was conducted between 8 January 2008 and 16 January 2008 by the Gallup Organisation. The target group was companies with 20 or more employees. In the UK 300 companies were sampled.

A survey conducted for the MoJ by British Market Research Bureau is also considered as part of the Equality Impact Assessment screening. This was conducted between 21 and 28 January 2010 and represents the views of 1,877 adults aged 15 or over in England and Wales. A similar survey conducted by ICM Research for the ICO has also fed into the Equality Impact Screening. This survey was carried out between 27 and 28 February and involved 1,004 adults over the age of 18 across England and Wales.

This IA also takes into account comments and evidence received from a wide variety of over 160 respondents to the Government's 2010 Call for Evidence on the Data Protection Legislative Framework, from Government Departments, Local Authorities, businesses, charities, consumer groups, and members of the public among others. Suggestions and 87 comments made on the Government's 'Your Freedom' website between July and September 2010 on data protection have also been considered.

Costs in hindsight

There is little firm evidence readily available about the full costs of implementation of the DPA. However, the PwC figures mentioned above provide a useful starting point for considering the administrative burdens placed on data controllers as a result of the DPA. As mentioned above, it should be noted that organisations may have incurred many of these costs voluntarily without the DPA. Therefore the extent to which we can allocate these costs solely to the DPA is difficult to establish.

Table 1 below shows the admin costs that different categories impose across the UK as a whole, including the important category of subject access requests (requests by individuals to find out from a data controller what personal data of theirs is being processed), broken down into its constituent elements:

Table 1

Administrative Cost	Cost per year (with "Business As Usual Costs" deducted) (£s)
Providing information (subject access requests): general	1m
Providing information (subject access requests): financial standing	41m
Providing information (subject access requests): education records	2m
Providing information (subject access requests): other burdens*	6m
Subject access total	50m
Notifying the Information Commissioner of activities	3m
Getting expert information from another party	Negligible
Total	53m

*For example, providing reasons why personal data cannot be disclosed.

These costs were calculated using the Standard Cost Model (<http://www.bis.gov.uk/policies/better-regulation/policy/simplifying-existing-regulations/reducing-administrative-burdens>) whereby costs are assessed on the basis of the average cost of an action (price) multiplied by the total number of actions performed per year (quantity). The average cost per action is estimated by multiplying a tariff (based on average labour cost per hour including prorated overheads) and the time required per action. For example, the costs for subject access requests are calculated on the basis that it takes between 10 and 75 minutes to process general subject access requests; around 80 minutes to process requests relating to financial standing; 85 minutes to process requests relating to education records; and between 30 and 90 minutes on other functions related to requests. It is estimated that the process of notifying the Information Commissioner takes between 20 and 40 minutes, and getting expert information from other parties takes between 50 and 90 minutes.

The total number of actions is estimated by multiplying the number of entities that have to fulfil an action by the frequency of that action. These results have been adjusted to reflect 2009 wage rates. Beyond the obvious costs borne by relevant sectors (banks for financial standing requests, credit reference agencies by credit reference requests, and schools and universities by education record requests), we have no further breakdown on which groups are affected by the above costs, although the Information Commissioner's Office's (ICO) response to the Call for Evidence noted that data controllers in the public sector received a higher volume of subject access requests than those in the private sector. This was

backed up by the figures provided by other respondents. In so far as business is concerned the Eurobarometer 226 survey noted that the number of subject access requests received was similar, regardless of their sector of activity.

A few respondents to the Call for Evidence acknowledged the difficulties in quantifying the administrative burdens, but believed that the figures mentioned above significantly underestimated the true cost of compliance with the DPA. The staff time required to deal with a subject access request varied considerably in responses depending on the nature of the business. The lowest time cited was 10 minutes for one member of staff, but in some cases a subject access request (SAR) required a small team working over a period of a month or more. The estimated cost of this compliance varied between £10 and several £10,000s per SAR, with most responses estimating an average of between £100 and £500. Again this disparity appeared to depend on the nature of the business and the systems in place to respond to such requests for personal data, rather than the sector of which the data controller was a member. There was no clear evidence to equate the cost of compliance with a SAR with whether the data controller was a public authority or a private company.

However, we recognise that respondents used different methods to calculate these costs and have taken differing types of cost into account when compiling these figures, making a more accurate cost impossible to quantify with certainty. The costs of SARs to business estimated by the Home Office in 1997 in its Regulatory Impact Appraisal were £302 million per year, which is significantly higher than the PwC figure above. This may reflect an over-estimation of the number of SARs that businesses would receive. Given that the PwC figures are the result of the most recent, comprehensive study of the DPA's administrative burdens, we use these estimates for the purpose of this IA, whilst acknowledging that there remains a large degree of uncertainty regarding the estimates.

Respondents to the Call for Evidence also reported a wide disparity in the volumes of subject access requests received. Some data controllers had received no subject access requests, or very few, while at the other end of the scale the UK Borders Agency reported receiving 700 requests per week, and the Association of Chief Police Officers Criminal Records Office (ACRO) receiving around 60,000 per annum. This evidence from the Call for Evidence is supported by the findings from the Eurobarometer 226 survey: 39% of UK sampled companies had never received any request in 2006; 37% had received fewer than 10 requests; 9% had received between 10 and 50 requests; and 5% had received more than 50 requests. Furthermore, companies with more than 250 employees were more likely to have received such requests than smaller companies. Not surprisingly, bigger companies reported receiving a larger number of requests than those in small and medium-sized companies. Again, this demonstrates that the size and nature of the business will generally dictate the volumes of subject access requests received. However, most respondents who discussed the issue were agreed that the volumes had increased in recent years as data subjects became more aware of their rights.

The main Credit Reference Agencies (Callcredit, Equifax and Experian) pointed out that, although they receive relatively few subject access requests under section 7 of the DPA, the requirement under section 9 to provide information on an individual's financial standing led to several million such requests per year. However, the nature of their business meant that the information was provided easily and automatically, with the cost of providing such information being around £5 per request.

There are almost certainly further burdens on data controllers imposed by the DPA. These costs are not quantified in this IA, although the Government acknowledges that they may be significant. Policy burdens could be in the form of extra staff hired to enforce compliance and raise awareness within the workplace on data protection matters. This awareness may be assisted by literature and training provided during staff induction. Fair Processing Notices, which are required to ensure compliance with the first data protection principle's requirement that personal data be processed fairly (see Schedule 1 to the DPA), will also impose a cost to businesses in terms of drafting and publication. In the Eurobarometer 226 survey, 69% of all respondents in the UK claimed that their company maintained and updated a privacy policy notice (in comparison to the EU average of 41%).

It is probable that organisations will have invested in software to protect the information they hold on individuals from misuse or theft. This would assist data controllers in complying with the seventh data protection principle that appropriate technical measures be taken against, amongst other things, unauthorised or unlawful processing of personal data. According to the Eurobarometer 226 survey, the proportion of UK respondents using privacy enhancing technologies to enhance protection of databases in their company has risen from 20% in 2003 to 39% in 2008. Furthermore, 85% of UK respondents said that their company takes measures to enhance the security of data transferred via the Internet whereas the EU average is only 67%. Any consideration of these policy costs should bear in mind "Business As Usual" (BAU) costs, i.e. those costs that data controllers would incur whether data protection legislation

existed or not. It is conceivable that some or all of the above measures would have been taken by businesses keen to provide a degree of assurance to customers that their personal data was safe.

Finally, there is a cost to the justice system as a result of the DPA, and the offences and enforceable rights it provides for. Cases can be heard in the Magistrates' Court, the Crown Court and the tribunals. These are considered in more detail in the Annex to this IA (see the 'Justice Impact Test').

Indicative benefits in hindsight

The quantifiable monetary benefits the DPA has brought are equally difficult to ascertain. Publications such as KPMG's 'Data Loss Barometer', the Ponemon Institute's Annual Study on data breach costs and the periodic InfoSecurity Information Security Breaches Survey do not set out the costs of compliance with the DPA, although we may assume that full compliance with the DPA would result in fewer data breaches occurring.

In its 2010 Information Security Breaches Survey, carried out by PwC, InfoSecurity Europe put the average business cost of the worst security breach at between £27,500 and £55,000 for a small organisation and between £280,000 and £690,000 for a large organisation. These costs include, among other things, investigating and responding to an incident, financial loss due to fraud, and damage to reputation. This study also found that 62% of large organisations and 35% of small organisations had a serious information security incident, although not all of these will necessarily have involved personal data. The tentative cost figure put forward overall for the UK by PwC and InfoSecurity Europe is in the order of several billion pounds. However, as with costs, it is difficult to establish whether data controllers would have established their own data protection policies and practices, even without the DPA. Therefore the extent to which we can allocate these benefits solely to the DPA is difficult to establish.

If we assume that the DPA prevents data breaches by providing a principles-based framework within which the processing of personal data takes place, as well as a regulatory system which provides for enforcement action in cases of non-compliance, we may assume there are some monetised benefits for the UK. If we assume that the DPA prevents between 25 and 50 data breaches across the UK every year (distributed among small organisations and large organisations, taking into account there are more smaller firms than larger firms), by using the InfoSecurity figures above, we can provide hypothetical assumptions for best-case and worst-case scenarios as set out in Tables 2 and 3 below:

Table 2

	Small organisation min (£s).	Small organisation max (£s).	Large organisation min (£s).	Large organisation max (£s).
1 data breach averted	27,500	55,000	280,000	690,000

Table 3

	Minimum	Maximum	Mean
Scenario 1 – 25 Data Breaches Averted (10 Large Firms, 15 Small Firms)	3m	8m	5m
Scenario 2 – 50 Data Breaches Averted (20 Large Firms, 30 Small Firms)	6m	15m	11m

These illustrative figures would suggest that the DPA saves UK businesses as a whole between £3m and £15m per year in terms of averted data breaches, with a mid-case scenario of £9m in savings. However, the figures presented are subject to significant uncertainty and, in particular, it is impossible to

determine the numbers of breaches that would take place if there were no DPA, and amongst which sizes of organisation these would be distributed.

Further to the above, businesses are assisted by the DPA in providing a framework in the UK which gives confidence to consumers that they can (for example) order goods online or join loyalty schemes, in the knowledge that their personal data is being held securely, and that the organisation in question will face repercussions if their information is misused. Equally, organisations in other countries will have increased confidence to trade and do business with UK-based companies, in the knowledge that their customers' information is secure. A small number of respondents to the Call for Evidence noted that robust data protection law properly applied was a factor in giving the UK a competitive advantage in some areas, particularly in credit referencing, which in turn is required for a successful financial services system. From the customer's point of view, individuals should have greater confidence that their personal data is being protected, and therefore may be more willing to provide information to organisations. This can allow the organisation concerned to offer more tailored goods and services and (for example) run loyalty schemes. However, despite these benefits being potentially considerable, we do not believe they are possible to quantify.

The legal framework has helped to increase confidence in the handling of individuals' personal data by creating a benchmark for the processing of personal data. The DPA has helped to safeguard individuals' rights to the protection of their personal data, in particular by providing for a means of redress for unfair or unlawful processing (either through the courts or the Information Commissioner). For example, in the financial year 2009-10 there were seven prosecutions for failure to notify as a data controller and two prosecutions for failure to comply with enforcement notices, with the ICO also serving 15 enforcement notices and securing 57 formal undertakings. By contrast, in 2008-9, there were 14 prosecutions for data protection offences, 10 prosecutions for failure to notify, and 20 enforcement notices and formal undertakings. This has resulted in non-monetised benefits for individuals, for example in being able to control the unsolicited mail they receive and in being able to view, correct and amend the information that commercial organisations hold on them.

Fines

Successful prosecutions under the DPA can result in fines being imposed, which are routed from data controllers and individuals to the consolidated fund (the central fund in which Government money is collected and distributed). In general, these fines are for not notifying the Information Commissioner of activities, and for crimes surrounding the misuse of personal data. Less often, fines have also been imposed for failure to comply with an enforcement notice served under section 40 of the DPA.

In the years between 2005 and 2010 these fines averaged around £10,000 per year from cases prosecuted by the ICO, although there is significant variation in the fines imposed in different years. For example, £23,200 in fines was imposed in 2005-06, while, by way of contrast the same figure in 2008-09 was £4,150. Annual costs awarded averaged around £9,000 in the same period. The Victim Surcharge introduced in 2007 yielded an average of around £100 for the years 2007/8 to 2009/10 for data protection offences prosecuted by the ICO.

There may be other data protection criminal cases we are unaware of that have been prosecuted by the Crown Prosecution Service, rather than the ICO, but these are believed to be relatively rare. The fines handed down for criminal offences set out below are considered for the purposes of this IA as benefits for the consolidated fund, but not costs for those data controllers and individuals who break the law. This is in line with standard IA methodology of not counting the costs to criminals.

In addition to fines, the ICO was given powers in 2010 to serve Civil Monetary Penalties (CMPs) of up to £500,000 on data controllers who commit serious breaches of the data protection principles. Respondents to the Call for Evidence believed that it was too early to assess the use of these penalties. After the Call for Evidence closed, the Information Commissioner served the first two CMPs in November 2010, one of £100,000 on Hertfordshire County Council and one of £60,000 on employment services company A4e. The IA published when the Government introduced CMPs made a central assumption that every year eight data controllers would each be served penalties of £100,000, resulting in £800,000 in penalties annually. However, we have not included the figures for civil penalties in this IA as a cost for data controllers and a benefit for the consolidated fund as these penalties have not been served for the vast majority of the time the DPA has been in force.

Awareness of information rights

Although hard to quantify, there is evidence from correspondence and from surveys commissioned by the ICO and the MoJ which indicates that the DPA has had a positive impact in terms of promoting awareness of data protection and wider information rights. In 2010, for example, 85% of respondents to the British Market Research Bureau's (BMRB) survey were aware of the right to find out what personal data was held by businesses or public authorities. Overall awareness of information rights is also underlined by ICO research which shows that information rights are amongst the most important social concerns: the protection of people's personal data ranked equal third with the NHS in an ICO survey of social concerns.

The BMRB surveys also demonstrate that awareness of the Freedom of Information Act 2000 (FOIA) is broadly on a par with awareness of the DPA, although the provisions of the two Acts are sometimes confused. The DPA gives individuals rights to access information held about them whereas the FOIA accords individuals the right to request access to official information held by over 100,000 public authorities. There are important exemptions in FOIA which relate to the processing of personal data. However, this overlap between the two Acts has created unintended consequences which can impact adversely on information rights. It should be noted that this does not stem from the DPA itself, but from the introduction of FOIA and the subsequent case law which relates to the aspects of the DPA that interact with section 40 of FOIA, (particularly in relation to the first data protection principle). Examples of the difficulties which this creates include:

- the DPA being presented as a technical barrier to openness, often noticeable in cases related to the disclosure of the names of public officials under FOIA. This arises from certain interpretations of condition 6 of Schedule 2 to the DPA which sometimes lead to a different outcome compared to considerations under the fairness test. In turn, these lead to outcomes of non-disclosure under FOIA, when disclosure would have no impact on an individual's private life;
- difficulties in interpreting the definition of personal data in conjunction with recital 26 of the Directive and suitable tests for deciding when information is "anonymised" in the context of Freedom of Information decisions and judgements.

Media organisations which responded to the Call for Evidence agreed with the view that the DPA could become a bar to openness, and noted their opinion that the DPA had had an impact on access to information. They argued that the DPA had become a barrier to reporting, investigation and publication as well as to maintaining archives.

Nonetheless, enhanced awareness of data protection has helped to raise the issue on the political agenda. Consequently, policies and initiatives with a data protection interest, such as CCTV, Government databases, and the use of biometrics to assert identity, have received more detailed scrutiny from the public, the media and Parliament.

Summary of the Review

Quantifying the costs and benefits of the DPA is difficult, due to the factors outlined above, and particularly due to the fact that comparison, either with the situation in the UK prior to 1984 or with countries with no data protection rules, is difficult. Equally, it is difficult to know what measures data controllers would take to protect the personal data they process if there was no data protection legislation in place (i.e. their BAU costs and benefits). The costs and benefits outlined above should therefore be treated as indicative, with the caveat that they are subject to much uncertainty.

Views of stakeholder and enforcement bodies on how well the DPA is meeting its objectives

The ICO's view is that the DPA has worked successfully for the most part.

Firstly, in terms of providing protection of personal data, the ICO believes that the level of protection afforded by the DPA is generally sufficient. Although it acknowledges that few of the obligations and financial burdens under the DPA would not otherwise be considered good business practice, it argues that high-profile breaches of data protection are a strong argument for the on-going need for a legal framework. It notes that such breaches have acted as a 'wake-up call' for some people as far as data protection matters are concerned, but that it is too soon to pass judgement on the effectiveness of their recent additional enforcement powers.

However, the ICO expresses some concern that the sanctions available against individuals who are involved in the unlawful trade of personal data are insufficient given the threat which they pose. In addition, it also identifies particular areas in which the legislation could provide greater clarity than at present, such as over the responsibilities of controllers and processors.

Secondly, the ICO believes that there has been success in terms of raising awareness about the use of people's personal data. Promoting the legislation, and the rights and responsibilities under the DPA, has encouraged a greater understanding of the role of personal data in everyday personal and corporate lives. This assertion is supported both by the rising level of complaints and enquiries with which they deal, as well as research which shows that people are increasingly concerned about their personal data and their control over it.

Respondents to the Call for Evidence largely expressed the view that the DPA was working well, but some respondents thought that the legal framework was ineffective. Particular concerns were raised by a few of those who responded about issues such as the transfer of personal data to third parties, the treatment of medical information and different approaches to gaining consent to processing personal data.

A smaller number of respondents felt that the DPA is too restrictive, and expressed concern that what they saw as its complexity has led to difficulties in effective implementation of the Act. Others thought that the DPA was overly bureaucratic and prescriptive, leaving data controllers with too little discretion over the way in which a particular outcome can be achieved.

The views of data subjects were extracted from a sample of correspondence received by the Ministry of Justice (and its predecessor, the Department for Constitutional Affairs) between January 2007 and April 2010. This sample consisted of 34 letters from MPs and 37 received directly from members of the public. It is not intended to be a scientific sample of the experiences of all UK citizens, but provides anecdotal evidence of the kinds of issues and difficulties encountered that can result at least in a perception that the DPA is flawed.

A large majority of correspondents were concerned with the rights of private companies to hold, use and share personal data. Particular concern was expressed about credit service companies holding outdated or incorrect personal data. Correspondents were confused and angry about the right of private companies to collect and hold personal data that was not directly supplied to that individual company.

Correspondents were also concerned about the often complex process that they had to undergo to get false personal data held about them corrected. They expressed a wish for harsher penalties to be imposed on companies who knowingly hold false personal data. However, we do not believe that such complaints are commonplace. According to the EU Barometer 226 survey, only 3% of respondents in 2008 answered that their company had received a complaint from individuals whose data was being processed. This is similar to the rate of complaint in 2003 (4%).

The definition of personal data was the subject of some confusion, especially in relation to new technologies. For example they questioned whether IP (Internet Protocol) addresses, mobile phone numbers and CCTV image stills constituted personal data. Correspondents were also concerned about the seemingly large amount of personal data that was available for view on the internet. They questioned whether greater control was needed over the publication of such data.

In many of the letters, the DPA was, or appeared to be, performing a blocking function when correspondents wanted to achieve a specific purpose. For example, where people with good intentions wanted to perform a specific action on behalf of a friend or relative, such as finding detail of a close friend's care in hospital, they were frustrated by the seemingly obstructive nature of the Act. Correspondents expressed disappointment that the DPA appeared to protect parties "in the wrong," such as tenants who did not pay their rent, at their own expense.

A large proportion of the correspondence sent directly to the department was from private companies, or individuals involved in the community, who were anxious for advice about their responsibilities under the DPA. Correspondents were keen for one clear source of advice to be established and publicised. Many individuals questioned the need to be registered under the DPA, and the associated charges involved with this. A high proportion of those correspondents who had written directly to the department either expressed frustration that they were not allowed to see personal data held about themselves, or wished to know how to make a SAR.

The correspondence received by the Department represents only a limited picture of how the DPA is working for most citizens. Given the scarcity of information on costs and benefits, there is the risk that the picture we have now is inaccurate.

Whether the policy is working as intended

In broad terms, the DPA is working as intended, with most challenges only arising in more limited or technical areas.

The DPA has provided a legal framework for the protection of personal data in the UK, providing individuals with certain rights and data controllers with certain responsibilities in relation to the processing of personal data. In particular, there seems to be broad support for the principles-based approach. Such an approach has been credited anecdotally with allowing the legal framework to be applied by different organisations to their own business.

There is also increasing awareness of the requirements and importance of data protection by both data subjects and data controllers. For example, the ICO's October 2010 track survey of social concerns showed that organisations' awareness of most of the DPA's data protection principles rose between 2009 and 2010. Organisations' awareness of individuals' rights to see information about themselves was at 89%. Individuals' awareness of the DPA is evidenced in particular by the growing number of individuals who refer enquiries or complaints about potential infringements of the DPA to the Information Commissioner (rising to over 32,000 in 2009-10, compared to 19,460 in 2004-5), as well as the administrative burdens borne by data controllers outlined above which illustrate the extent to which organisations comply with the law, especially in relation to notification and subject access obligations. In 2009-10, there was a further year-on-year rise in the number of registered data controllers, taking the total to 328,164.

However, evidence received in response to the MoJ's Call for Evidence, correspondence from MPs and the public to the Department, the media and elsewhere suggests that there is not universal understanding or correct application of the DPA. This means that, in certain areas, the processing of personal data may still be open to abuse or misuse. The perceived complexity of the DPA has on occasion been held up as a reason not to comply proactively with the law or the reason why a breach has occurred, for example confusion over who constitutes the data controller amongst several organisations or what constitutes personal data. This complexity was mentioned repeatedly by respondents to the Call for Evidence as a reason why the DPA was not being applied correctly. Some consumer groups have also said that there is anecdotal evidence of widespread non-compliance with the Act among data controllers, and that recourse to the courts when the DPA was breached was too costly for most data subjects.

In relation to the other main intention of the Directive - harmonising minimum standards of data protection across the European Economic Area (EEA) -, transposing the Directive through the DPA has brought the UK closer in line with other Member States. However, Member States have implemented the Directive in different ways, leading to a level of variation between Member States.

Respondents to the Call for Evidence highlighted such variations in relation to the eighth data protection principle (on international transfers). In particular, they cited the different approaches taken by other EU Member States in satisfying the requirements for international data transfers. They said that some supervisory authorities required large amounts of detailed information before transfers outside of the EEA could take place, while others took a more streamlined approach. This process could often take months, or in one particular case, years to complete. They also said that the low number of 'adequacy' decisions by the European Commission (the process by which non-EEA countries are deemed to have sufficient data protection standards in place) was a key concern and called for more work in this area. Respondents also found the need to register with each supervisory authority to be burdensome, given that the requirements varied wildly between different Member States in the amount and type of information required. They suggested that a single process covering all Member States would be preferable.

Application of the DPA

There have also been negative consequences arising from enhanced awareness of data protection. Notably, it has given rise to instances of misapplication of the Act by data controllers, often documented in the media, who fail to disclose or share personal data, citing the DPA as the reason, even when this processing would be harmless and legitimate. This can often be a result of a lack of understanding about the DPA's requirements, which leads to an over cautious approach to the disclosure of personal data. This has sometimes created unnecessary barriers in practice to the processing of personal data which were not intended by the legislation (or indeed which are not provided for in the legislation). Examples of this range from the more trivial, such as parents being prevented from taking photos of their children in

school plays, to very serious cases such as that highlighted by the Birchard Inquiry into the Soham murders. In the latter, Sir Michael Birchard noted the initial citation of data protection legislation as a bar to sharing vital information, a proposal which the report rejected.

Respondents to the Call for Evidence pointed to a variety of circumstances in which the DPA appeared to be a barrier to useful and legitimate data sharing, although again they stressed that this was often due to an over-cautious approach to data protection. For example, academics, landlords, social researchers, insurers and investigators pointed out that the DPA was used as a reason not to disclose personal data, even where exemptions within the Act allowed it. Several respondents mentioned the issue of data protection preventing valuable medical research from taking place, and this is considered in the 'Health and Wellbeing Impact Test' section below.

Many respondents to the Call for Evidence mentioned that a very large proportion of subject access requests were received in the context of litigation and employment disputes. In some cases, it was believed that data subjects' legal representatives were using subject access requests as a cheap and easy means of disclosing information earlier than it would otherwise be in the course of legal proceedings. It was suggested that this was an abuse of the original intentions behind providing individuals with the right of subject access.

Annexes

Annexes may be added to provide further information about non-monetary costs and benefits from Specific Impact Tests, if relevant to an overall understanding of policy options.

Equality Impacts

Statutory Equality Duties Impact Test

The Data Protection Act 1998 (DPA) has had no perceivable impact on equality. An Equality Impact Assessment Review is attached.

Economic Impacts

Competition Assessment Impact

The introduction of the DPA may have affected the ability of micro, small and medium sized firms to enter new markets, or compete in existing markets (see also Small Firms Impact Test). For example, the DPA's requirements may mean that firms have decided not to store customer data and so are missing out on the benefits of customer profile marketing.

Additionally, the DPA may affect UK firms' ability to enter and compete in international markets where personal data protection legislation has not been introduced, or is less stringent.

Firms who comply with DPA measures may be affected if they have to compete against other businesses that do not comply with the DPA, and so have lower administrative costs.

It is also possible that the safeguards in the DPA may engender consumer confidence and brand loyalty amongst individuals, thereby providing firms with a competitive advantage over organisations not subject to comparable data protection laws (for example in some third countries outside the EEA).

Small Firms Impact Test

The DPA has had an impact on all firms which collect and process personal data. The introduction of regulation in this area has involved staff time to understand the provisions of the DPA and its implications for their business.

In a small firm (10-49 employees) or micro firm (1-9 employees) it is more likely that it will fall to the business owner or other senior personnel to understand and enforce regulatory responsibilities, meaning staff time costs will be higher. Additionally, it is less likely that small firms will have the resources to pay for independent legal advice to inform them of their obligations under the DPA.

Respondents to the Call for Evidence pointed out that an increase in volumes of subject access requests (for example, in response to a complaint or negative media story) can result in small firms facing difficulties in responding to requests within the statutory deadline, with the limited staff numbers finding it hard to cope with the increased workload.

According to the EU Barometer 226 Survey, across the EU:

- more small companies (20-49 employees) (32.8%) were unfamiliar with the provisions of data protection law than medium-sized companies (49-250 employees) (27.7%) and large companies (over 250 employees) (17%);
- the usage of privacy enhancing technologies was less widespread in small companies (47%) than medium-sized (58%) and large companies (70%);
- small companies (45%) were less likely to receive subject access requests compared to large ones (51%);
- 5% of small companies received more than 50 subject access requests per year compared to 13% of large ones;
- 36% of small companies said their company updated privacy policies compared to 62% of large ones.

From these figures it would appear that the DPA does not disproportionately affect small firms, although the impact of future changes to the legislation on them will need to be carefully considered.

Environmental Impacts

Greenhouse Gas Assessment

The DPA has had no identifiable impact on greenhouse gasses.

Wider Environmental Issues

The DPA has had no identifiable impact on the wider environment.

Social Impacts

Health and Wellbeing Impact Test

There is the potential for a very slight impact on public health in relation to the sanctions that can be imposed under the DPA. The threat of significant penalties, additional work, financial burdens and the perceived complexity of the DPA could cause mental health impacts such as anxiety and stress to those who have to work with personal data. This could have an impact especially on those who work in front line services and have to make vital and often complex decisions about whether to disclose personal data, while taking account of the DPA's requirements.

In addition, respondents to the Call for Evidence from the medical profession also pointed out that the DPA has acted as a barrier to medical research, as it is not always possible to anonymise medical data fully when carrying out research. It may be that, in turn, this has had an indirect health impact on individuals, but no evidence on this has been put forward. Bodies representing adopted people also mentioned that the data protection rights granted to biological parents have meant that vital genetic information has been withheld from those who are adopted.

The DPA may also impact on partnership working if its safeguards result in a reluctance to share personal data between services such as the health services, the police and other emergency services (as discussed above – see page 13). This could conceivably present consequences for the type, timeliness and quality of care, though no firm evidence was submitted on this in response to the Call for Evidence.

However, despite these concerns, no further evidence was provided in response to the Call for Evidence to suggest that the potential direct impact upon public health and wellbeing is significant enough to conduct a full health and wellbeing impact test.

Human Rights Impact Test

The DPA has had a significantly positive effect upon matters related to Article 8 of the European Convention on Human Rights – the right to respect for private and family life. This right means that everyone has the right to respect for private and family life, their home and their correspondence.

Personal data is protected as part of an individual's right to private life enshrined in Article 8. Any disclosure of personal data to another person or the collection and storage of personal data is likely to constitute an interference with a right to private life under Article 8.

The DPA has enhanced public understanding of the importance of protecting personal information and the impact on the individual of unauthorised disclosure of this information.

Judicial interpretations of the Human Rights Act 1998 have extended the right to a private life within a home to include also the right to a private life within a place of business in specific circumstances. This may apply to microfirms and sole traders who operate from their homes. The DPA includes the right for inspection of business premises without consent either under an assessment notice, or under warrant powers contained within Schedule 9 to the Act. This could lead to a potential conflict between Article 8 and the DPA. However, we believe that the powers of entry and inspection of the Information Commissioner are proportionate, necessary and come with appropriate rights of appeal so that any interference would be justified.

Finally, media organisations have argued that data protection rights have conflicted with rights under Article 10 of the Convention – the right to freedom of expression. As discussed above, it has been reported that data protection has been given as a reason to refuse personal data to journalists investigating news stories in the public interest. However, it should be noted that the DPA sets out exemptions for the purposes of journalism, literature and art, and the Article 10 right to freedom of expression is a qualified one, which needs to be balanced against other rights (for example, the right to respect for private and family life)

Justice Impact Test

Data controllers can be prosecuted under the terms of the DPA which leads to an inevitable impact upon the justice system. Generally, the DPA's requirements are enforced by the ICO, which has estimated its annual enforcement costs for 2009-10 at around £1m.

Due to the offences introduced under the DPA, magistrates courts, county courts and tribunals will have experienced an increase in caseload with the DPA being enforced both by the ICO and through private prosecutions. This workload will also include the collection and enforcement of those fines and penalties imposed under the DPA, and specialist judicial training on the provisions of the DPA.

The DPA may have created the possibility of more legal challenges due to two key factors. These are:

- that the DPA, like the Directive, contains broad principles for data processing that allow for interpretation by individual data controllers. This ability to apply a degree of personal discretion may have increased the number of times that potential infringements of the DPA are challenged in the courts;
- that the DPA has attracted a high level of public interest, which means that the likelihood of litigation is higher.

We know that since 2005 the ICO has brought prosecutions against 71 individuals (as of May 2010). However, it may be that more than one individual was involved in one case. From figures provided by the ICO in its annual reports for 2005/6 to 2008/9 there was an average of eight hearings per year in the magistrates courts, with only one Crown Court case being heard in this period (in 2005). In 2007, two cases were heard in the Scottish courts. Further, in the same period, the Information Commissioner applied to a circuit judge for a warrant for entry and inspection under Schedule 9 to the DPA on average 9 times per year. Since the DPA came into force in 2000, 15 enforcement cases have gone to the Tribunal, an average of 1.5 every year. From these figures we have assumed that approximately 10 court hours per year are spent on data protection offences. Seen within the context of around 1 million judicial hours used each year, it is clear that the DPA has had a minimal impact on the justice system.

The rights and offences created under the DPA have an impact on legal aid budgets.. However, the figures for the civil legal aid budget for 2008-09, collated as part of the MoJ's review 'Proposals for the Reform of Legal Aid in England and Wales' indicate that legal aid awarded for civil cases involving data protection was negligible. Similar figures for criminal cases were unavailable, but again, given the small numbers of data protection cases prosecuted, this is thought to be low.

Rural Proofing Impact Test

The DPA has had little perceivable impact on rural communities.

However, rural businesses are more likely to be small or micro firms, and accordingly will be affected as discussed under the Small Firms Impact Test.

In addition, it is likely that local town and parish councils will similarly be affected more by the administrative costs of complying with the DPA than their larger counterparts. These costs may include additional temporary staffing in order to comply with data protection legislation relating to Subject Access Requests or notification to the ICO.

As with small firms, in small councils these responsibilities may also be more likely to fall to senior personnel meaning staff-time costs will be higher. Additionally, it is less likely that town and parish councils will have the resources to pay for independent legal advice regarding their obligations under the DPA.

Stakeholders agreed however that these factors did not amount to more than a marginal impact on rural communities.

Sustainable Development Impacts

Sustainable Development Impact Test

The DPA has had no identifiable impact on sustainable development.