

**Title:**

Proposal for an EU Data Protection Regulation

**IA No:****Lead department or agency:**

Ministry of Justice (MoJ)

**Other departments or agencies:**

Department for Culture, Media and Sport (DCMS)

Home Office (HO)

Information Commissioner's Office (ICO)

**Impact Assessment (IA)****Date:** 22/11/2012**Stage:** Development/Options**Source of intervention:** EU**Type of measure:** Other**Contact for enquiries:** Ollie Simpson**Summary: Intervention and Options****RPC Opinion:** Awaiting Scrutiny**Cost of Preferred (or more likely) Option**

Total Net Present Value	Business Net Present Value	Net cost to business per year (EANCB on 2009 prices)	In scope of One-In, One-Out?	Measure qualifies as
£2,100m	£1,700m	£130m	No	Zero net cost

**What is the problem under consideration? Why is government intervention necessary?**

There has been data protection law within Europe since the 1970s. This has involved certain key elements, such as the right of access to one's own personal data and to have automated decisions reviewed, and the responsibility on organisations to process personal data fairly and lawfully. The 1995 EU Data Protection Directive (95/46/EC) dates from 1995 and is aimed at reconciling the protection of personal data with the free flow of data within the internal market. However, since 1995, there have been numerous technological developments, notably the expansion of the internet and the emergence of social media. The EU Commission believes that the law should be updated to reflect these changes and to provide more harmonisation across EU Member States.

**What are the policy objectives and the intended effects?**

The aims of the EU Commission's proposal are to update current data protection legislation, taking into account the growth in the processing of personal data over the last seventeen years as well as a perceived lack of harmonisation in Member States which the Commission contends has produced barriers for data controllers in the internal market. The proposals also aim to cut administrative burdens, whilst reinforcing consumer confidence by strengthening individuals' data protection rights with a series of new provisions. These include more stringent requirements on those organisations which process personal data.

**What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)**

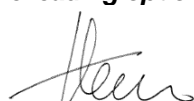
This Impact Assessment evaluates the key costs and benefits of the proposed Data Protection Regulation, as published on 25 January 2012.

**Will the policy be reviewed?** It will not be reviewed. **If applicable, set review date:** Month/Year

Does implementation go beyond minimum EU requirements?			N/A		
Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base.	<b>Micro</b> Yes	<b>&lt; 20</b> Yes	<b>Small</b> Yes	<b>Medium</b> Yes	<b>Large</b> Yes
What is the CO <sub>2</sub> equivalent change in greenhouse gas emissions? (Million tonnes CO <sub>2</sub> equivalent)			<b>Traded:</b> N/A		<b>Non-traded:</b> N/A

***I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.***

Signed by the responsible Minister:



Date: 22/11/2012

# Summary: Analysis & Evidence

## Policy Option 1

Description:

### FULL ECONOMIC ASSESSMENT

Price Base Year 2012	PV Base Year 2012	Time Period Years 14 (10 years from introduction)	Net Benefit (Present Value (PV)) (£m)		
			Low: -£900	High: -£3,200	Best Estimate:--£2,100

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	Optional	£210	£1,800
High	Optional	£580	£5,100
Best Estimate		£400	£3,500

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

The following costs to business have been monetised: requirement to employ a data protection officer (DPO), requirement to carry out data protection impact assessments (DPIAs), requirement to notify all personal data breaches to the supervisory authority, and the administrative cost of demonstrating compliance. Monetised costs to the public sector include the expanded role of the supervisory authority, the loss of notification fee income, the requirement to employ a DPO and demonstrating compliance.

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

Data portability and the 'right to be forgotten' are expected to be costly for data controllers to implement. The Regulation also introduces a higher standard for obtaining consent, tighter restrictions on profiling, and less flexibility on international transfers, which could be costly for UK data controllers. Large fines are expected to be costly to business as they are disproportionate to the harm caused and may therefore lead to firms spending more than is necessary on data protection compliance.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	Optional	£110	£900
High	Optional	£220	£1,900
Best Estimate		£160	£1,400

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

Monetised benefits to business include reducing legal fragmentation of data protection law across the EU, a reduction in the loss of personal data and savings from no longer having to notify with the supervisory authority. There is also a benefit to individuals who no longer have to pay for Subject Access Requests.

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

Enhanced protection of personal data is a benefit to individuals who are less likely to be victims of identify fraud and can have more confidence sharing their data online. This may also have a knock-on economic benefit if it leads to an increase in the use of internet services. The Regulation also gives individuals greater control over their personal data through measures such as 'the right to be forgotten', and data portability.

#### Key assumptions/sensitivities/risks

Discount rate (%)

3.5

The costs and benefits of the data protection proposals have been calculated as average annual figures. Costs and benefits are based on current wages/prices multiplied by the number of activities/organisations affected by the proposals, and have been up-rated in line with earnings for future years where this is appropriate. The Regulation is expected to come into force in 2016-17 and so costs and benefits have been projected forward over 10 years from this date. The main assessment is based on full compliance with the proposals.

### BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) -£130m			In scope of OIOO?	Measure qualifies as
Costs: £100m	Benefits: £230m	Net: -£130m	No	Zero net cost

## Table of Contents

Chapter 1:	Key figures in Impact Assessment	4
Chapter 2:	Background	5
	Problem under consideration	5
	Affected groups	6
	Rationale for intervention	6
	Policy objective	6
	Government commitment	6
	Scope	7
Chapter 3:	Principles of the cost benefit analysis	8
	Base case	8
	Analytical principles	8
	EU Commission's figures	9
	Impact of Regulation	9
Chapter 4:	Monetised costs and benefits	12
Chapter 5:	Direct costs and benefits to business calculations (following OIOO methodology)	25
Chapter 6:	Non-monetised costs and benefits	25
Annexes		
	Annex A - Underlying data	32
	Annex B - Small Medium Enterprises (SME) impact	35
	Annex C - Competition impact	40
	Annex D - Justice impact	44
	Annex E – Equality Impact Test	49

## Evidence Base (for summary sheets)

### 1. Key Figures in Impact Assessment

Table 1.1 gives the breakdown for the annual costs and benefits presented in this Impact Assessment, shown over the 14 year appraisal period. Where figures grow over time, this is due to the effect of earnings up-rating. Table 1.1 shows that in 2016-17, the year the Regulation starts to apply, the proposals are expected to have a net cost of £250 million. A 14 year appraisal period has been used as the policy has been appraised over 10 years from the year of introduction, 2016-17.

**Table 1.1: Cost and benefits of the mid-range estimate (£millions; 2012 prices)**

	2012-2016	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26
<b>Benefits</b>											
Reduction in legal fragmentation	£0	£40	£50	£50	£50	£50	£50	£50	£50	£50	£50
Reduction in data breaches	£0	£100	£100	£100	£100	£110	£110	£110	£110	£120	£120
No Notification	£0	£20	£20	£20	£20	£20	£20	£20	£20	£20	£20
SAR Fees (individual)	£0	£10	£10	£10	£10	£10	£10	£10	£10	£10	£10
ICO	£0	£1	£1	£1	£1	£1	£1	£1	£1	£1	£1
<b>Total Benefit</b>	<b>£0</b>	<b>£170</b>	<b>£170</b>	<b>£180</b>	<b>£180</b>	<b>£180</b>	<b>£180</b>	<b>£190</b>	<b>£190</b>	<b>£190</b>	<b>£200</b>
<b>Costs</b>											
Notifying breaches	£0	£90	£90	£90	£90	£90	£100	£100	£100	£100	£100
SAR Requests	£0	£30	£30	£30	£30	£30	£30	£30	£30	£30	£30
DPIAs	£0	£80	£80	£80	£80	£90	£90	£90	£90	£90	£100
DPOs	£0	£160	£160	£170	£170	£180	£180	£180	£190	£190	£200
ICO	£0	£40	£40	£40	£40	£50	£50	£50	£50	£50	£50
Demonstrating Compliance	£0	£30	£30	£30	£30	£30	£30	£30	£30	£30	£30
<b>Total Cost</b>	<b>£0</b>	<b>£420</b>	<b>£430</b>	<b>£440</b>	<b>£450</b>	<b>£460</b>	<b>£470</b>	<b>£480</b>	<b>£490</b>	<b>£500</b>	<b>£510</b>
<b>Net Benefit</b>	<b>£0</b>	<b>-£250</b>	<b>-£260</b>	<b>-£260</b>	<b>-£270</b>	<b>-£280</b>	<b>-£280</b>	<b>-£290</b>	<b>-£300</b>	<b>-£300</b>	<b>-£310</b>

*Note: figures have been converted to 2012 prices using the GDP deflator. Figures have been rounded to the nearest £10million and so totals may not always sum.*

Table 1.2 shows the figures in table 1.1 once discounting has taken place; figures have been discounted back to 2012-13. In net present value terms the cost in 2016-17 is £220 million. The total net present value over the 14 year appraisal period is -£2.1 billion.

**Table 1.2: Discounted costs and benefits of the mid-range estimate (£millions; 2012 prices)**

	2012-2016	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26
<b>Discounted Benefits</b>											
Reduction in legal fragmentation	£0	£40	£40	£40	£40	£40	£40	£40	£40	£40	£30
Reduction in data breaches	£0	£80	£80	£80	£80	£80	£80	£80	£80	£80	£80
No Notification	£0	£20	£20	£10	£10	£10	£10	£10	£10	£10	£10
SAR Fees (individual)	£0	£8	£7	£7	£7	£6	£6	£6	£5	£5	£5
ICO	£0	£1	£1	£1	£1	£1	£1	£1	£1	£1	£1
<b>Present Value Benefit</b>	<b>£0</b>	<b>£150</b>	<b>£150</b>	<b>£140</b>	<b>£140</b>	<b>£140</b>	<b>£140</b>	<b>£130</b>	<b>£130</b>	<b>£130</b>	<b>£130</b>
<b>Discounted Costs</b>											
Notifying breaches	£0	£70	£70	£70	£70	£70	£70	£70	£70	£70	£70
SAR Requests	£0	£20	£20	£20	£20	£20	£20	£20	£20	£20	£20
DPIAs	£0	£70	£70	£70	£70	£70	£60	£60	£60	£60	£60
DPOs	£0	£140	£140	£140	£140	£130	£130	£130	£130	£130	£130
ICO	£0	£40	£40	£40	£40	£30	£30	£30	£30	£30	£30
Demonstrating Compliance	£0	£20	£20	£20	£20	£20	£20	£20	£20	£20	£20
<b>Present Value Cost</b>	<b>£0</b>	<b>£370</b>	<b>£360</b>	<b>£360</b>	<b>£350</b>	<b>£350</b>	<b>£340</b>	<b>£340</b>	<b>£330</b>	<b>£330</b>	<b>£320</b>
<b>NPV</b>	<b>£0</b>	<b>-£220</b>	<b>-£220</b>	<b>-£210</b>	<b>-£210</b>	<b>-£210</b>	<b>-£210</b>	<b>-£200</b>	<b>-£200</b>	<b>-£200</b>	<b>-£200</b>

*Note: figures have been converted to 2012 prices using the GDP deflator, and then discounted using a discount rate of 3.5%. Figures have been rounded to the nearest £10million and so totals may not always sum.*

## 2. Background

### **Problem under consideration**

The data protection landscape has changed since the 1970s, where EU citizens were not subjected to the increased level of data processing, which is now common place. The rise in the level of data processing has been largely due to the increased processing power of computers and the potential for automated decision-making both in the public and private sectors. At the heart of data protection legislation have been certain key rights, such as the right of access to one's own personal data, the right to rectify inaccurate personal data, the right to have personal data deleted under certain circumstances, and the ability to have automated decisions reviewed. Equally the law has placed obligations on organisations to process personal data fairly and lawfully; to specify the purposes for which personal data is processed; and the need to put proper security measures in place. These elements were set out in the first internationally binding data protection instrument, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108') 1981.

The 1995 EU Data Protection Directive (95/46/EC) established a framework for data protection amongst EU Member States. However, since 1995, there have been numerous technological developments, notably the increased use of personal computers and, more recently, handheld devices; the rapid expansion of the internet; and the emergence of social media. The EU Commission believes that the law should be updated to reflect these changes and to provide more harmonisation across EU Member States. Respondents to a UK Government Call for Evidence in 2010<sup>1</sup> generally believed the existing legislation was sound, although some did agree that the law needed to be updated to reflect technological change.

Further to a period of consultation between 2009 and 2011, the Commission published two proposals for the protection of personal data on 25 January 2012. The proposals feature a draft Regulation and a draft Directive. The Regulation would apply to general data processing by the public and private sectors, whilst the Directive is intended to cover the former third pillar areas of police and criminal justice.

Alongside the publication of the proposals, the Commission published its Impact Assessment on the costs and benefits the proposals would have on Member States. The Commission estimated that the new regime would bring a net administrative benefit totalling €2.3 billion to the EU each year, mostly due to a harmonised data protection regime. However, the Government believes the Commission has overestimated the benefits from one single law and has failed to take into account many of the new compliance costs in its headline figure by focusing purely on administrative burdens.

This Impact Assessment aims to present a fuller summary of the costs and benefits of the proposals and their wide ranging impacts on affected sectors of society in the UK.

### **Affected Groups**

The Regulation will impact on all organisations ('data controllers' and 'data processors') established in the EU. It will also apply to organisations which are not established in the EU if those organisations process the personal data of data subjects residing in the EU when offering them goods or services or monitoring their behaviour. The Regulation will apply to the following groups of organisations established in the UK:

- public sector data controllers and processors including government departments, local authorities, and non-departmental public bodies.
- private sector data controllers and data processors: including large multinational corporations, micro, small and medium businesses, and sole traders. It will have a greater impact on those organisations whose business depends heavily on the processing of personal data such as credit reference agencies, banks, and information society service providers.
- civil society: including charities and voluntary organisations.

---

<sup>1</sup> Responses to the Call for Evidence on the Current Data Protection Legislative Framework, 28 January 2011, p7

It is estimated that there are approximately 355,000 data controllers that will be affected by the Regulation, 54% of which are private sector businesses. This is based on the number of organisations notifying with the UK supervisory authority and so will exclude data controllers that fail to notify or are exempt. The breakdown for these figures is given in Annex A.

The Regulation will also affect people whose personal data is processed by EU organisations and EU residents whose personal data is being processed by non-EU organisations ('data subjects') by continuing to protect their personal data by law. Individuals whose personal data is being processed ('data subjects') are given a number of rights in relation to their data. Those rights may be asserted, directly against the data controllers (or sometimes processors). Data subjects may complain to the supervisory authority about the processing of their data, and may also seek a judicial remedy where their rights have been infringed. They also benefit from strengthened rights of access, portability, deletion and rectification with respect to their personal data. The proposals will therefore impact on UK citizens in other Member States, and the wider world, and they will also apply to Gibraltar.

The proposals would also impact on the supervisory authorities in each Member State. For the UK, the Information Commissioner is the designated supervisory authority. Widening the scope of the supervisory authority's responsibilities and powers will require substantially more resources, for example undertaking prior authorisation, greater cooperation with supervisory authorities in other Member States, and the potential for more litigation involving the supervisory authority.

There will also be an impact on the justice system if the proposals lead to more data protection cases being brought.

### **Rationale for intervention**

In addition to the technological innovation and growth in the use of personal data set out above, the EU Commission contends that a lack of trust in online services is deterring individuals from taking up goods and services, both from the public and private sectors. It claims that "If not addressed this lack of confidence will continue to slow down the development of innovative uses of new technologies, to act as an obstacle to economic growth and to block the public sector from reaping the potential benefits of digitisation of its services, e.g. in more efficient and less resource intensive provisions of services." In addition, the Commission claims that a lack of harmonisation across the EU is leading to legal uncertainty and a "widespread" perception that online transactions pose privacy risks<sup>2</sup>.

The UK welcomes a revision to data protection law. However, the Government would like to see a data protection framework that will stimulate economic growth and innovation, whilst providing data subjects with a proportionate level of protection.

### **Policy objective**

The policy objective for the UK is to achieve an EU data protection framework that will protect the personal data of individuals while allowing for economic growth and innovation. This framework should facilitate the exchange of personal data between Member States, thereby improving the operation of the internal market and also address the impact of new technologies. However, the MoJ's recent Call for Evidence highlighted the need to scrutinise the proposals' impact on business, the public sector, the consumer and the economy at large. Respondents to the Call for Evidence were mainly from the business sector, and have raised broadly similar concerns, believing that the proposed legislation could stifle economic growth and innovation<sup>3</sup>.

### **Government Commitment**

In recognition of the concerns expressed by businesses about the cost of administrative and compliance burdens in these proposals, the Government committed in its summary of responses to its Call for Evidence on the EU data protection proposals that it would resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals.

---

<sup>2</sup> Commission's Impact Assessment, p7

<sup>3</sup> Summary of Responses to Call for Evidence on Proposed EU Data Protection Legislative Framework (2012)

Reducing the regulatory burden on business is vital for economic growth and job creation. The Government has taken considerable steps to reduce regulatory burdens arising from national legislation (through, for example, the One-in, One-out rule and Red Tape Challenge). It is also determined to minimise the cost to business of legislation from Brussels.

The EU institutions have supported better (or 'smart') regulation for several years. They recognise the importance of consultations and of conducting impact assessments and then having regard to the financial implications of proposals (2003 inter-institutional agreement on better law-making). The European Commission has made specific commitments to reduce the cost of EU regulation on business, including through a joint target to reduce administrative burdens by 25% by 2012. It also recently pledged to minimise EU regulatory burdens on SMEs, and specifically listed these data protection proposals as ones where it would aim to respect the "Think Small First" principle. In its Small Business Act, it commits to supporting Europe's SMEs and to improve the regulatory environment for them.

We do question whether the data protection proposals have taken into consideration the Heads of Government agreement to reduce administrative burdens and the general consensus of affected sectors that these proposals would have a negative impact on economic growth.

## **Scope**

This Impact Assessment aims to evaluate the impact of the Commission's proposals as published on 25 January 2012 on UK private sector data controllers and, where possible, the impact on public and civil society data controllers. It also considers the impact on data subjects and, to a lesser extent, the impact on processors. The detail of these proposals is subject to negotiation in the Council and European Parliament, so the final draft may be different from the proposal. Indeed, the UK is pushing for a less prescriptive, more flexible approach to regulation in this area. In addition, there is provision for Member States to introduce national legislation in certain areas. The European Commission has also proposed giving itself numerous powers to make delegated and implementing acts some of which deal with very significant areas, which would again affect the costs and benefits of the new data protection framework. However, this Impact Assessment assumes that the proposals are to come into effect as drafted, and does not take account of the provision for Member States and the Commission to bring forward further legislation.

This Impact Assessment focuses on the proposed Regulation. Under Article 6A of the UK's Title V Opt-In Protocol we believe that the proposed Directive will have a limited effect on the United Kingdom, in that it will only apply to data being processed under an EU instrument that binds the UK. Therefore, criminal justice system agencies within the UK will avoid being bound by the Directive when processing personal data outside of such provisions.

It is worth noting that organisations which process criminal justice data will also process personal data covered under the Regulation and so some of the monetised costs and benefits stemming from the Regulation could be shared (for example, the cost of designating a data protection officer). The Directive would require transposition into UK law, at which point domestic legislation would also be needed to cover that processing purely internal to the UK. There is therefore a degree of flexibility for Member States in determining how the EU-level rules in the proposed Directive would be transposed and a fuller assessment of the costs and benefits specific to the proposed Directive will be produced nearer the point of transposition.

Importantly, the cost-benefit analysis which follows is not an exhaustive one. There may be further provisions in the proposed Regulation which will have a potentially significant impact, as well as opportunity costs. We have identified what we see as the main burdens and savings.

### **3. Principles of the Cost Benefit analysis**

The next section sets out the 'base case': the assumptions the Government has made about future trends if none of the changes set out in the data protection proposals are implemented and if there is no change in policy practice. It then proceeds to set out the analytical principles adhered to, before summarising briefly the impact assessment carried out by the EU Commission and why the UK does not agree with this assessment. The main cost-benefit analysis of many of the provisions in the proposal follows; each section briefly presents an assessment, where the evidence permits, of the estimated costs and benefits to affected parties, although the latter section also deals with costs and benefits that we are unable at present to monetise.

#### **Base case**

The existing EU data protection instrument is the 1995 Data Protection Directive 95/46/EC, implemented into UK law by the Data Protection Act 1998 (DPA). The DPA is regulated by the UK Information Commissioner's Office. The base case assumes that this data protection legislative framework would continue in its current form. The Government's estimate of the costs and benefits of this to the UK are set out in its Post Implementation Review Impact Assessment, published in January 2011.

The base case assumes that, in the absence of the Regulation, the number of businesses and other organisations processing personal data will remain unchanged going forwards and that the number of data protection breaches will remain unchanged. While we may expect to see some increase in the number of organisations collecting and processing personal data over the coming years this is not possible to project with any certainty. The assumptions underpinning the number of affected organisations, both public and private, are set out in Annex A.

#### **Analytical Principles**

This Impact Assessment aims to identify, as far possible, the impacts of the proposals on society. A critical part of the process is to undertake a cost benefit analysis of the proposals. The cost benefit analysis assesses whether the proposals would deliver a positive impact to society, accounting for economic, social and logistical considerations.

The Impact Assessment has focused on key monetised and non-monetised impacts. It is not practical to undertake a forensic assessment of the proposals and so the impact assessment restricts itself to some broad elements of the Regulation. Although the Regulation is likely to change as a result of negotiations, for the purpose of this assessment it has been necessary to assume that the Regulation as drafted will be adopted.

The evidence informing the figures in the Impact Assessment is based on desk-research, responses to the Call for Evidence on the proposals, and additional consultation that has taken place with data controllers and representatives of data subjects. We have also engaged directly with the EU Commission to better understand their Impact Assessment analysis. The costs to the Information Commissioner's Office (ICO) have been calculated separately by the ICO and provided to the MoJ. Given the variability in the costs and benefits to different types of controllers it is not possible to estimate the costs and benefits precisely and so where appropriate costs and benefits have been presented as ranges.

The key monetised impacts are calculated as average annual figures which are projected to grow over time in line with earnings inflation. While we would expect organisations to look to reduce additional cost burdens over time by changing their behaviour where possible, the uncertainty in this means it has not been possible to model this behavioural change. However, this does mean that some caution should be observed when considering costs and benefits several years into the implementation of the Regulation.

The monetised costs and benefits are based on the assumption that data controllers comply with the Regulation. However, the monetised costs and benefits section does assume that breaches of personal data will occur as now, as breaches will occur for many reasons, such as a theft, and are not necessarily the result of an organisation breaching its obligations under the DPA.



## The EU Commission's figures

The EU Commission has used the 'Standard Cost Model' approach to model the administrative burden of the proposals. This approach only includes "administrative activities that businesses are required to conduct in order to comply with the information obligations of the Regulation". It doesn't include other policy costs or compliance costs, or costs to the public sector. The Standard Cost Model approach is a recognised approach for quantifying administrative burdens. However, in the UK we would argue that policy costs also need to be included in order to measure the full economic impact of the Regulation.

The EU Commission's Impact Assessment<sup>4</sup> estimates that the proposals will lead to a reduction in administrative burdens for business of €2.3 billion per annum. This is made up of a saving of €2.9 billion from harmonisation of data protection rules, minus a cost of €580 million for businesses to demonstrate compliance with the Regulation and a cost of €20 million from notifying data protection breaches to the supervisory authority.

The EU Commission Impact Assessment does acknowledge that there will be additional compliance costs, focusing on DPOs, DPIAs and additional costs to supervisory authorities in the main assessment. However, no attempt is made to quantify the total net benefit of the Regulation to take account of these costs.

It is the view of the Ministry of Justice that the EU Commission headline saving of €2.3 billion is too high, for the following reasons:

- 1. Benefits are over-estimated:** the EU Commission estimate of savings from reducing legal fragmentation (€2.9 bn / £2.3 bn) can be considered an upper-bound estimate because it is based on the assumption that just over 900,000 businesses face compliance costs of €1,000 p.a (£800) for every additional Member State in which they are established. There are only 42,000 large businesses in the EU and evidence from the Federation of Small Business suggests that smaller businesses are less likely to face costs from legal fragmentation<sup>5</sup>. The harmonisation methodology is explored in more detail in the monetised costs and benefits section.
- 2. Policy costs are not included:** the EU Commission Impact Assessment fails to quantify key policy/compliance costs and additional costs to the public sector, such as data protection officers. For the UK alone, the requirement for data controllers to employ data protection officers and carry out data protection impact assessments are together estimated to cost £130-£320 million p.a. in 2012/13 earnings terms.
- 3. Administrative costs are under-estimated:** The EU Commission estimates that only 1,000 additional data breaches will be notified to supervisory authorities; giving an administrative cost of €20 million (£16 million). However, survey evidence suggests that 45% of large UK companies and 11% of small companies have at least one breach per year<sup>6</sup>. For the UK alone, reporting breaches is estimated to cost £30-£130 million p.a. in 2012/13 earnings terms. The cost of dealing with additional Subject Access Requests that will arise from the removal of the fee is also excluded.

## Impact of the Regulation

This assessment of the proposals has focused on addressing the impacts relative to the base case. In doing so, it has been necessary to devise criteria to guide the assessment given the detailed and varied nature of the proposals. This impact assessment has focused on those policies which: are likely to have a relative significant impact (positive or negative) on the UK; may be of important public debate; and, may have been raised by stakeholders in response to the UK's Call for Evidence.

---

<sup>4</sup> European Commission (2012), Impact Assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

<sup>5</sup> In its evidence to the UK Justice Select Committee the Federation of Small Businesses stated that of its members "very few will export data, so the savings from harmonisation are very small". 2012

<sup>6</sup> PWC (2012), 'Information security breaches survey: technical report'.

Based on the above criteria, the main policy areas assessed are:

#### *Monetised costs and benefits*

- Reduction in legal fragmentation: the Commission states that differences in implementation of the 1995 Directive have led to fragmentation, legal uncertainty and inconsistent enforcement, and therefore has proposed a new Regulation to address these issues.
- Reduction in personal data breaches: the intended outcome of the Regulation is that organisations better protect personal data through taking a proactive approach to data security. This is expected to reduce the loss of personal data.
- Personal data security breach notifications: the proposal sets out a requirement for data controllers to notify the supervisory authority of all personal data breaches, without undue delay, and within 24 hours where this is feasible.
- Removal of notifications: the proposals will abolish the current system of notification. Currently data controllers must notify the Information Commissioner of their data processing activities and pay a fee.
- Data protection officers (DPOs): the proposal sets out a requirement that data controllers must designate a data protection officer if: they are a public body; or have more than 250 employees; or their core activities including processing operations which require regular and systematic monitoring of data subjects.
- Data protection impact assessments (DPIAs): the proposal sets out a requirement that data controllers or processors must undertake a data protection impact assessment on data processing which presents specific risks.
- Subject access requests (SARs): the Commission proposes making subject access requests exercisable free of charge. It also proposes widening the amount of information that data controllers must provide and sets a time limit of a month to comply with a request.
- Supervisory authority role and powers: the proposals include new, specific requirements for supervisory authorities to provide mutual assistance to each other. This is intended to ensure that the Regulation is implemented and applied in a consistent manner.
- Demonstrating compliance (including maintaining documentation): the Commission proposes a general obligation on data controllers to demonstrate compliance with the data protection legislation. Compliance can come in various forms, such as showing that a data protection impact assessment has been carried out.

#### *Non-monetised costs and benefits*

- Data portability: the proposal sets out a new right to data portability, which gives individuals the right to obtain from the data controller a copy of their data in an electronic and structured format which is commonly used and which allows for further use by the data subject.
- Right to be forgotten: the proposal sets out a new right to be forgotten, including the right for data subjects to obtain erasure of personal data relating to them and the abstention from further dissemination of such data.
- International transfers: the proposals build on the existing mechanisms and provide a detailed framework for transfers of personal data outside of the European Economic Area (EEA). There are also requirements for a supervisory authority to undertake prior checks of some types of transfers, including those based on contractual clauses.
- Restrictions on Profiling: the proposals build on Article 15(1) of Directive 95/46 (automated individual decisions). The proposals have taken into account the Council of Europe's recommendation on profiling and give data subject's rights not to be subject to a measure based on profiling.
- Consent: the Regulation sets out that consent must be "explicit". This represents a higher threshold for consent, compared with the 1995 Directive. Further conditions about when consent is an acceptable grounds for processing personal data are set out (in article 7).

- Administrative sanctions: the proposals include a three-tier system of administrative sanctions for a wide range of infringements of the Regulation. The highest sanction available to supervisory authorities is either €1,000,000 or 2% of an enterprise's annual worldwide turnover.

*Other possible costs and benefits*

- Data minimisation: the proposals set out requirements for data controllers that personal data be 'limited to the minimum necessary' (in Article 5(c)). This would mean that data controllers would have to remove as many identifiers as possible from the data they process, in order to ensure that it constitutes the minimum amount of data necessary in relation to the purpose for which they are processed.
- General obligations on data processors: the proposals introduce specific requirements on data processors if they are asked to carry out a processing operation on behalf of the controller.
- Transparent information and communication: the proposals place an obligation on the controller to provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject.
- Certification: Member States and the Commission will encourage the establishment of data protection certification mechanisms and data protection seals and marks which will allow data subjects to assess the level of data protection provided by controllers and processors.

The figures in the Impact Assessment are based on the assumption that the annual costs continue into the future. However, in practice we would expect controllers to adapt their processes in order to reduce the administrative burden imposed by the Regulation and Directive. This behavioural impact is not accounted for in this Impact Assessment.

## 4. Monetised costs and benefits

The monetised costs and benefits of the data protection proposals have been calculated as average annual figures. Costs and benefits are based on current wages/prices multiplied by the number of activities/organisations affected by the Regulation, and so represent an annual cost in 2012-13 earnings terms. These costs have been uprated in line with forecast earnings growth for future years, where this is appropriate.

The annual costs and benefits of the Regulation are shown in Table 4.1. The Regulation is expected to lead to a net cost of between £100 and £360 million per annum in 2012-13 earnings terms. Table 4.1 also shows the projected annual cost just to the private sector; the expected cost to business of the proposals is between £80 million and £320 million per annum in 2012-13 earnings terms. A detailed assessment of how these figures have been calculated is given below.

**Table 4.1: Annual costs and benefits of the Regulation (£millions; 2012-13 earnings terms)**

	Average Annual (£millions)					
	Total			Business only		
	Low	Best/Mid	High	Low	Best/Mid	High
<b>Benefits</b>						
Reduction in legal fragmentation	£20	£40	£70	£20	£40	£70
Reduction in data breaches	£60	£90	£120	£60	£90	£120
No Notification	£20	£20	£20	£10	£10	£10
SAR Fees (individual)	£10	£10	£10	n/a	n/a	n/a
ICO	£1	£1	£1	n/a	n/a	n/a
<b>Total Benefit</b>	<b>£110</b>	<b>£160</b>	<b>£220</b>	<b>£90</b>	<b>£140</b>	<b>£200</b>
<b>Costs</b>						
Notifying breaches	£30	£80	£130	£30	£80	£130
SAR Requests	£10	£20	£40	£10	£20	£40
DPIAs	£70	£70	£80	£70	£70	£80
DPOs	£60	£150	£240	£50	£140	£230
ICO	£20	£40	£40	n/a	n/a	n/a
Demonstrating Compliance	£20	£20	£50	£10	£20	£40
<b>Total Cost</b>	<b>£210</b>	<b>£400</b>	<b>£580</b>	<b>£170</b>	<b>£340</b>	<b>£520</b>
<b>Net Benefit</b>	<b>-£100</b>	<b>-£230</b>	<b>-£360</b>	<b>-£80</b>	<b>-£190</b>	<b>-£320</b>

Note: figures have been rounded to the nearest £10 million and totals may not always sum.

The Regulation is not expected to be implemented until 2016-17. Table 4.2 shows the net present value of the Regulation over the next 14 years, based on the mid-range estimates in table 4.1. As the majority of activities in table 4.2 are staff activities, the cost of these activities has been increased in line with forecast earnings growth. However, the number of organisations/activities affected has been held constant since it is not possible to project how the number of data controllers/businesses in the UK may change over the next fourteen years.

Table 4.2 shows that the net present value of the Regulation is -£220 million in 2016-17, the year of introduction. The net present value of the Regulation over the next fourteen years is -£2.1 billion.

**Table 4.2: Present value costs and benefits of the mid-range estimate (£millions; 2012 prices)**

	2012-2016	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26
<b>Discounted Benefits</b>											
Reduction in legal fragmentation	£0	£40	£40	£40	£40	£40	£40	£40	£40	£40	£30
Reduction in data breaches	£0	£80	£80	£80	£80	£80	£80	£80	£80	£80	£80
No Notification	£0	£20	£20	£10	£10	£10	£10	£10	£10	£10	£10
SAR Fees (individual)	£0	£8	£7	£7	£7	£6	£6	£6	£5	£5	£5
ICO	£0	£1	£1	£1	£1	£1	£1	£1	£1	£1	£1
<b>Present Value Benefit</b>	<b>£0</b>	<b>£150</b>	<b>£150</b>	<b>£140</b>	<b>£140</b>	<b>£140</b>	<b>£140</b>	<b>£130</b>	<b>£130</b>	<b>£130</b>	<b>£130</b>
<b>Discounted Costs</b>											
Notifying breaches	£0	£70	£70	£70	£70	£70	£70	£70	£70	£70	£70
SAR Requests	£0	£20	£20	£20	£20	£20	£20	£20	£20	£20	£20
DPIAs	£0	£70	£70	£70	£70	£70	£60	£60	£60	£60	£60
DPOs	£0	£140	£140	£140	£140	£130	£130	£130	£130	£130	£130
ICO	£0	£40	£40	£40	£40	£30	£30	£30	£30	£30	£30
Demonstrating Compliance	£0	£20	£20	£20	£20	£20	£20	£20	£20	£20	£20
<b>Present Value Cost</b>	<b>£0</b>	<b>£370</b>	<b>£360</b>	<b>£360</b>	<b>£350</b>	<b>£350</b>	<b>£340</b>	<b>£340</b>	<b>£330</b>	<b>£330</b>	<b>£320</b>
<b>NPV</b>	<b>£0</b>	<b>-£220</b>	<b>-£220</b>	<b>-£210</b>	<b>-£210</b>	<b>-£210</b>	<b>-£210</b>	<b>-£200</b>	<b>-£200</b>	<b>-£200</b>	<b>-£200</b>

*Note: figures have been converted to 2012 prices using the GDP deflator, and then discounted using a discount rate of 3.5%. Figures have been rounded to the nearest £10million and so totals may not always sum.*

The rest of this section sets out the evidence for the monetised costs and benefits and explains how the figures have been calculated. The headline figures, presented above, have been rounded to the nearest £10 million due to the uncertainty surrounding the estimated costs and benefits of the Regulation. However, in the next section the unit costs and benefits are presented to the nearest £1 million in order to demonstrate clearly how the main figures have been calculated and how the total cost and benefits have been reached.

#### Reduction in legal fragmentation (benefit)

Private sector data controllers that operate in more than one Member State currently incur costs through having to comply with the data protection laws of other member states – referred to by the EU Commission as legal fragmentation. The Regulation aims to remove some of these costs by having one data protection law for all Member States (harmonisation), although legal fragmentation will still exist as the Regulation provides for Member States to introduce national legislation in certain areas. Legal fragmentation is estimated here using the methodology adopted by the EU Commission in its Impact Assessment.

The EU Commission estimates the cost of legal fragmentation to be €5,000 (£4,000) for every additional Member State that a business operates in; this cost is repeated every five years and so the annual cost is €1,000 (£800)<sup>7</sup>. This cost consists of €2,000 (£1,600) translation costs, €2,500 (£2,000) legal validation work, and €500 (£400) clerical work. The number of organisations affected is estimated by taking the number of private sector data controllers and using EU Barometer survey evidence to estimate the number operating within other EEA Member States. For the UK, this is a quarter of private sector data controllers – giving a total of 48,000 data controllers affected<sup>8</sup>. Following the methodology of the EU Commission, this number is then halved on the basis that under Data Protection Directive 95/46/EC a data controller is affected by the data protection legislation of another Member State if they are “established” in that other Member State and processing is done in the context of that other establishment<sup>9</sup>.

The €5,000 (£4,000) cost is not just incurred once, but is repeated for every Member State the organisation operates in. For the UK, survey data shows that 11% of firms operating in another Member State operate in just one other member state, 13% operate in two or three and 76% operate in at least four<sup>10</sup>. In total then, the cost to UK businesses of legal fragmentation is £66 million in 2012-13 earnings terms using the EU Commission methodology.

<sup>7</sup> EU Commission Impact Assessment. Annex 9, page 145.

<sup>8</sup> EU Commission (2011), ‘Retailer’s attitudes towards cross-border trade and consumer protection’. Flash Barometer Survey 300.

<sup>9</sup> There is no justification given in the EU Commission Impact Assessment for ‘halving’ being a good measure of ‘established’.

<sup>10</sup> EU Commission (2011), ‘Retailer’s attitudes towards cross-border trade and consumer protection’. Flash Barometer Survey 300.

However, evidence from the EU Commission SME Panel finds that only 27% of businesses, to whom the question was applicable, had paid for legal advice on data protection issues<sup>11</sup>. If only 27% of data controllers affected by legal fragmentation pay for legal advice then the unit cost of legal fragmentation falls to €3,182 (£2,545). This reduces the total present cost to UK businesses to £42 million. This is the mid-point estimate of the benefit of harmonisation.

There is an alternative way to approximate the number of organisations “established” in another Member State other than halving the number of controllers operating overseas. The EU Barometer survey provides estimates of the number of organisations with a “retail outlet or subsidiary” in another Member State, giving a rough approximation for the number of controllers that could be affected by legal fragmentation<sup>12</sup>. This reduces the proportion of data controllers affected by legal fragmentation to 8% and reduces the number established in multiple Member States to 32% in one other Member State, 10% in two or three and 58% in at least four. This reduces the overall current cost of legal fragmentation to £22 million. However, this is considered the lower bound estimate as “established” is slightly wider than just having a “retail outlet or subsidiary” in that Member State, but can refer to any means of processing located on the territory of an EU Member State.

The cost of legal fragmentation will apply to private sector data controllers only, and has been up-rated annually in line with forecast earnings growth. A summary of the key figures is given in table 4.3 below:

**Table 4.3: Summary of annual savings from reducing legal fragmentation; 2012-13 earnings terms**

	<b>Low</b>	<b>Best</b>	<b>High</b>
Controllers in 1 Member State	4,793	2,588	2,588
Controllers in 2 Member State	1,534	3,163	3,163
Controllers in 4 Member State	8,627	18,403	18,403
Unit Cost p.a.	£509	£509	£800
<b>Total Cost (£million)</b>	<b>£22</b>	<b>£42</b>	<b>£66</b>

An important factor to bear in mind is that the proposals as drafted do not equate to full harmonisation in any case. Several important elements are still left for national law, for example, Article 21 allows Member States to restrict the scope of obligations and rights provided for under many of the provisions in Chapters I-III. Therefore, it is unlikely that firms will be able to eliminate the need to seek legal advice on the legislation in different Member States.

#### Reduction in personal data breaches (benefit)

It is intended that by implementing the Regulation, organisations will take a more proactive approach to data protection which should reduce the amount of personal data that is lost or stolen. This could be achieved through measures such as requiring organisations to carry out data protection impact assessments which allow controllers to identify risk and take measures to reduce them, and by requiring controllers to implement appropriate technical and organisational measures for processing (article 23).

A 2009 survey carried out by Accenture found that organisations which regularly monitored privacy and data protection were 26% less likely to have had a data protection breach compared with organisations that did not regularly monitor privacy and data protection<sup>13</sup>. The survey carried out by Accenture also found that, of organisations which had at least two breaches, 41% of them did not regularly monitor privacy and data protection. Therefore, it is possible that if the Regulation is successful in getting organisations to take a more proactive approach to data protection the proportion of breaches could fall by 26% for 41% of organisations, leading to an overall reduction in data breaches of 11%.

<sup>11</sup> EU Commission Impact Assessment. Annex 8, page 138. The SME Panel surveyed 383 SMEs across the EU on their current data protection obligations. This is a small sample of SMEs and so the results should be treated with some caution

<sup>12</sup> EU Commission (2011), ‘Retailer’s attitudes towards cross-border trade and consumer protection’. Flash Barometer Survey 300

<sup>13</sup> Accenture (2009), ‘How global organisations approach the challenge of protecting personal data’. A survey of businesses found that 49% of organisations that don’t regularly monitor privacy and data protection had a data breach compared to 36% of organisations that do.

A 2012 survey of UK businesses, carried out by Infosecurity, found that 11% of small businesses and 45% of large businesses had an incident in the past year where data protection laws/regulations were breached<sup>14</sup>. Applying these figures to the number of data controllers registered with the UK's Information Commissioner would mean around 22,600 breaches occurring each year: around 2,000 large and around 20,600 small. This data will only include a company's worst incident, since the same survey showed that the vast majority of companies have more than one incident a year. An 11% reduction would reduce the number of breaches to 20,220 per annum, assuming that the number of breaches remains unchanged over-time in the absence of the Regulation.

The loss of personal data can be very costly to business, due to business disruption, direct and indirect financial loss, and damage to reputation. The same survey, carried out by Infosecurity, estimated the cost of security breaches to be between £15,000-£30,000 for an SME and £110,000-£250,000 for a large business. The Ponemon Institute estimated that the average breach cost £1.68 million in 2009, with an average cost per record lost of £64<sup>15</sup>. Comparison with the Infosecurity data suggests that the Ponemon research is focused on very large breaches and so the Infosecurity estimates have been used for this analysis. Based on the figures estimated by Infosecurity, an 11% reduction in personal data security breaches would lead to savings for business of £58-£124 million per annum in 2012-13 earnings terms, depending upon the cost of the breach. These savings are expected to grow in line with average earnings. A summary of the savings is given in table 4.4 below, the mid-point of the range, £91 million, is considered the best estimate of the savings.

**Table 4.4: Annual savings from reducing the loss of personal data; £millions 2012-13 earnings terms**

	Breaches Reduced	Savings (£millions)
<b>SMEs</b>	2,265	£34 - £68
<b>Large Enterprises</b>	223	£25 - £56
<b>Total</b>	<b>2,488</b>	<b>£58 - £124</b>

This benefit has only been estimated for the private sector.

#### Notification of Personal data security breaches (cost)

Article 31 of the proposed Regulation requires that all personal data breaches must be reported to the Information Commissioner without undue delay and, where feasible, within 24 hours. Currently, there is no general obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, although such a requirement has been introduced for Communications Service Providers under the revised e-Privacy Directive (2002/58/EC). However, serious breaches can be reported voluntarily to the Information Commissioner. 603 breach notifications were reported to the Information Commissioner from all sectors in 2010-11<sup>16</sup>.

#### *Private Sector*

When looking at just the worst incident for an organisation, approximately 22,500 data protection breaches occur each year (see previous section). As this will only include a company's worst incident it is a good proxy for the number of breaches that will be reported each year under the Regulation; however, if all breaches were reported, as the Regulation sets out, the true number and cost could be even higher. Taking account of the 11% reduction that is expected to occur from businesses implementing the Regulation (estimated above), leaves around 20,220 breaches that will need to be reported to the supervisory authority.

The additional cost to business of notifying a breach involves collating the information for the supervisory authority, reporting the breach and acting upon the response from the supervisory authority, plus the financial loss to the company as a result of the breach being made public. We estimate the cost of

<sup>14</sup> PWC (2012), 'Information security breaches survey: technical report'. 447 organisations were surveyed.

<sup>15</sup> Ponemon Institute, LLC (2010), 2009 Annual Study: cost of a data breach.

<sup>16</sup> Information Commissioner's Office (2011). Information Commissioner's Annual Report and Financial Statements 2010/11.

notifying a breach to cost between £1,000 and £2,000 depending upon the scale of the breach. This includes initial incident analysis and fact finding, drafting the letter to the supervisory authority, and analysis and response to replies and questions from the supervisory authority. However, this estimate is considered to a minimum and in some cases the cost will be considerably higher as there is often much back and forth between the controller and the ICO when examining a breach.

PWC survey data estimates the 'damage to reputation' from a security incident to cost a small business £100 - £1,000 and a large organisation £5,000 - £40,000. Adding these figures to the cost of reporting gives a total cost from notification of £1,100 - £3,000 for a small organisation and £6,000- £42,000 for a large organisation. Multiplying these costs by the additional number of breaches gives a total cost of between £31 million and £131 million per annum in 2012-13 earnings terms, and so the best estimate is the mid-range of these values: £81 million p.a. However, costs could be higher if organisations are expected to implement additional measures as a result of the breach. A summary of the key annual costs is given in table 4.5 below.

**Table 4.5: Annual cost of reporting data security breaches for the private sector; 2012-13 earnings terms**

		<b>Low</b>	<b>Mid Point</b>	<b>High</b>
<b>Additional cost of notification</b>	<b>SME</b>	£1,100	£2,050	£3,000
	<b>Large Enterprise</b>	£6,000	£24,000	£42,000
<b>Total Cost (£millions)</b>	<b>SME</b>	£20	£38	£55
	<b>Large Enterprise</b>	£11	£43	£76
<b>Total (£millions)</b>		<b>£31</b>	<b>£81</b>	<b>£131</b>

The number of breaches reported is assumed to be constant over time since it is not possible to know what would happen to the overall number of breaches in the absence of the Regulation. The cost of notification is projected to go up in line with average earnings growth.

The requirement to notify within 24 hours could have cost implications for businesses. In response to the UK's Call for Evidence on the proposals a number of respondents stated that it took more than 24 hours to investigate the breach and collate the necessary information to give to the Commissioner; for example, BT reported that it takes at least 72 hours to report a breach. The 24 hour rule is likely to mean breaches being hurriedly investigated. This could reduce costs if investigations are less thorough, although could lead to additional costs if the investigation needs to be repeated.

### *Public Sector*

NHS bodies and central government are already obliged to report serious breaches to the ICO<sup>17</sup>. In 2010-11, 165 breaches were reported by the NHS and 32 by central government. There will be additional costs under the new proposals, given that there is no threshold proposed on the face of the instrument as drafted on the severity of breaches that need to be reported. However, as there is limited data available on the total number of breaches that occur in the public sector as a whole it is not possible to quantify these additional costs.

### Removal of notification requirement (benefit)

Under the proposed Regulation, data controllers will no longer need to notify the data protection supervisory authority of their processing activities. The ICO reports its estimated fee income to be £15,600,000 for 2012-13<sup>18</sup>. Therefore, removing the notification fee gives a saving to data controllers (and a loss to the ICO) of approximately £15.6 million per annum. This is projected to remain constant since it is not known, either what will happen to the number of controllers or the level of the fee going forwards. This will include both public and private sector data controllers.

<sup>17</sup> ICO (2011), 'Information Commissioner's annual report and financial statements 2010/11'.

<sup>18</sup> [http://www.ico.gov.uk/about\\_us/our\\_organisation/key\\_facts.aspx](http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx); accessed: 14/11/2012



Data controllers will also see a small saving from the administrative burden of completing the annual notification form. In 2005 PWC estimated the cost of this burden to be £12.50 (in 2012-13 earnings terms) per data controller. Multiplying this by the number of data controllers in the UK gives a total saving of £4.4 million from no longer having to notify, the private sector makes up 54% of this saving (£2.4 million). This savings only includes the cost of completing the notification form, since controllers will still be required to maintain similar documentation under article 28 of the proposal. This cost will go up in line with earnings.

#### Demonstrating compliance (cost)

Article 22 of the Regulation imposes a general obligation on data controllers to demonstrate compliance with data protection law. The EU Commission's Impact Assessment estimates that the need to demonstrate compliance costs €200 (£160) per organisation, based on four hours of clerical work. This cost is intended to capture all additional administrative obligations on the controller, which include:

- Maintaining documentation of all processing activities (article 28);
- Maintaining documentation of data protection impact assessments that are carried out (Article 33) and documentation on the data protection officer (Article 35);
- Obtaining prior authorisation from the supervisory authority for processing (article 34).

The EU Commission's Impact Assessment estimates that this is an activity which needs to be repeated every three years giving an annual cost of £53. There are 355,000 data controllers registered with the UK supervisory authority, and based on the EU Commission methodology demonstrating compliance is estimated to cost £19 million p.a. in 2012-13 earnings terms, covering both public and private sector controllers.

However, for large organisations and small organisations carrying out 'regular and systematic' processing the cost of demonstrating compliance with the Regulation is expected to be far higher than £53 a year. Article 28 requires that each processor and controller needs to maintain documentation on all processing activities unless they employ fewer than 250 people and process personal data only as an activity 'ancillary to its main activities'.

For large organisations and smaller businesses classified as carrying out 'risky' processing in annex A, updating this documentation is an activity which will need to be repeated far more often than once every three years. At a minimum, these activities will need to be repeated once a year, giving a cost of £160 per annum to demonstrate compliance. However, for many controllers documentation on processing will need to be continually updated. Therefore, as an upper-bound the cost of repeating these activities is assumed to be once a quarter, or £640 per annum.

There are 6,000 large data controllers and around 42,000 smaller organisations that are expected to face this higher cost of demonstrating compliance with the Regulation. The unit cost and total cost for different controllers under the three scenarios is set out in table 4.6 below. The best estimate of the cost is £24 per annum in 2012-13 earnings terms, assuming that small controllers only update their processing information once every three years and large controllers or controllers carrying out regular processing do this once a year. However, the table shows that the costs could be higher if this documentation needs to be updated more regularly, giving an upper bound estimate of £47 million per annum.

**Table 4.6: Annual Cost of demonstrating compliance (2012-13 earnings terms)**

	Unit Cost		
	Low	Best	High
<b>Small Controllers</b>	£53	£53	£53
<b>Large/Controllers carrying out regular processing</b>	£53	£160	£640
	Total Cost (£millions)		
<b>Small Controllers</b>	£16	£16	£16
<b>Large/Controllers carrying out regular processing</b>	£3	£8	£31
<b>Total</b>	<b>£19</b>	<b>£24</b>	<b>£47</b>

Using the same methodology the cost to business is estimated to be between £10 million and £38 million per annum in 2012-13 earnings terms. This is based on the assumption that there are 4,500 large data controllers and that the 42,000 small controllers processing risky data are all private sector controllers.

### Subject Access Requests (SARs) <sup>19</sup>

Article 12 of the Regulation requires that subject access requests (SARs) and other rights are to be exercisable “free of charge” by the data controller. This is a cost to data controllers who can currently charge a £10 fee for SARs. Administering the fee generally costs more than £10, and so the loss of the £10 fee is not considered a cost. For example, the MoJ (as a data controller) estimates the cost of administering the £10 SAR cheque to be £20. The cost to business from this article arises from the rise in SARs that occurs as a result of the removal of the fee.

However, in the case of educational records and health records a maximum fee of £50 can be charged. In these cases no longer being able to charge a fee will result in a loss of income for these bodies.

It is difficult to estimate the cost of answering a SAR since this will vary for different controllers:

- in 2005 PWC estimated the average cost of a SAR to be £45 (measured in 2012-13 earnings terms)<sup>20</sup>;
- the 2011 Post Implementation Review of the Data Protection Act estimated a SAR to cost between £100 and £500. In response to the UK’s 2012 Call for Evidence, Mobile Broadband Group reported this estimate to be correct;
- the British Retail Consortium estimate the average cost to be £50, while accepting that the cost can be higher in some cases;
- In the Call for Evidence International Financial Data Services reporting receiving around 20 SARs a year, each which costs £550-£650

In this Impact Assessment, a range of **£50-£100** has been used as the cost of responding to a SAR. £50 is the lower bound, as this is the figure estimated by PWC and supported by the British Retail Consortium. £100 has been used as the upper bound, as this is the lower bound of the range reported in the Post Implementation Review of the Data Protection Act. While in some cases costs will be higher than £100, it seems reasonable to use this range since it is expected that the increase will be focused on organisations already receiving a lot of SARs and therefore likely to have a system in place to answer them as efficiently as possible. This cost does not include the cost of administering the £10 fee, which is assumed to be offset by the fee itself.

The volume of SARs has been estimated using the EU Flash Barometer 226 survey<sup>21</sup>. The survey found that 5% of UK private organisations receive more than 50 SARs a year, with 2% receiving 100+ and 1% receiving 500+. The survey only included companies employing at least 20 people. Using the 2011 Business Population estimates it is possible to calculate the number of organisations receiving at least

<sup>19</sup> This refers to Article 12: Information to the data subject

<sup>20</sup> The PWC administrative burdens have been increased in line with Average Weekly Earnings.

<sup>21</sup> EU Commission (2008), ‘Data protection in the European Union: data controller’s perceptions’. Flash Barometer 226.

50 SARs a year. This data is given in table 4.7. It shows that approximately 4,600 private sector organisations receive over 900,000 SARs each year. The mid-point of each band has been used to calculate the number of SARs.

**Table 4.7: Proportion of businesses receiving SARs and number received**

	Number of SARs per company			Total
	50-100	100-500	500+	
<b>Number of Companies</b>	2,713	904	1,005	4,621
<b>Number of SARs</b>	203,442	226,046	502,325	931,813

*Source: EU flash barometer survey 226 and BIS 2011 Population Estimates. SAR estimate is based on the mid-point of the range: 75, 250, 500.*

Table 4.7 is likely to slightly underestimate the total number of SARs as the survey data is from 2006 and the table excludes companies receiving less than 50 SARs. The PWC research from 2005 estimated the total number of SARs to be 1.17 million. However, it seems appropriate to use this lower measure given that a) evidence received from organisations is that the number of SARs has increased over the years<sup>22</sup> and b) the focus is on those companies likely to experience an increase in requests and so likely already to receive a significant number.

### *Benefits*

The removal of the £10 fee is a benefit to individuals making SARs. Taking the PWC data and EU survey data together suggests that individuals in the UK make at least a million SARs each year. This is a benefit to the individual of £10 million per annum. This saving will remain constant over time, since we assume that the possibility of charging a £10 fee would not change in the absence of the Regulation.

### *Costs*

The additional cost to business depends on the increase in SARs. There is no loss of income from the removal of the fee, since this is offset by the cost of administering that fee.

One large organisation responding to the Call for Evidence estimated that the volume of SARs could increase by 40%. This was based on 92 SARs which were not followed up when the £10 fee was requested, compared with 229 requests which were answered.

However, an alternative way to estimate the impact on SAR volumes is to look at the impact of introducing charges in other countries. In 2003 Ireland introduced a charge for FOI requests which led to a reduction in requests of around 30%<sup>23</sup>. Similarly, introducing a fee in Ontario led to a reduction in FOI requests of around 20%<sup>24</sup>. Reversing these figures gives an increase of 25%-43%<sup>25</sup>. These figures include both non-personal and personal requests, the equivalent of SARs. In Ireland, the fall in non-personal requests was larger than the fall in personal requests, but these figures give an indication of the potential rise that may be incentivised by the removal of the fee, particularly when the focus is on those organisations already receiving large number of requests.

Table 4.8 shows the additional cost to business of a rise in SARs of between 25% and 40%, based on a cost of £50-£100 per SAR. It shows that costs could be between £12 and £37 million depending on the extent of the increase. These costs would be expected to increase in line with average earnings growth.

<sup>22</sup> Paragraph 23 - Response to the Call for Evidence on the Current Data Protection Legislative Framework, from 06/07/10 to 6/10/10

<sup>23</sup> Office of the Information Commissioner (2005). Annual Report 2004.  
<http://www.oic.gov.ie/en/Publications/AnnualReports/2004/File,15925,en.pdf>

<sup>24</sup> Frontier Economics (2006), Independent review of the impact of the Freedom of Information Act.

<sup>25</sup> Ontario received 26,316 requests in 1995 before the introduction of the fee, and 20,788 in 1996 after its introduction. Based on these figures, removing the fee would lead to a rise of 25%.

**Table 4.8: Additional cost to business from increased SAR volume; £million per annum**

	<b>25%</b>	<b>40%</b>
<b>Additional SARs</b>	232,953	372,725
<b>Cost</b>	£12 - £23	£19 - £37

*Private Sector (Credit reference agencies)*

Under section 9 of the Data Protection Act (DPA), credit reference agencies have an obligation to provide copies of consumer credit files on request from data subjects. These requests are received in their thousands each day and millions each year across the three main credit reference agencies (Equifax, Experian and Callcredit).

As a result of the nature of their business and the fact that there is growing understanding amongst UK consumers of the need to be aware of their credit file (supported by the UK Government as it encourages greater financial probity) a charge of £3-£4 is placed per credit file request. This charge covers the cost of providing a comprehensive pool of credit information in an understandable format for the data subject, averting any follow up queries. Credit reference agencies will therefore also be particularly affected by no longer being able to charge a fee.

It has also been argued that requesting an appropriate contribution from the individual is a critical component in deterring fraudsters from attempting to obtain high volumes of credit file data. If data access upon request were to become free of charge then individuals would face an increased risk of frauds (e.g. account takeover) with its attendant detrimental consequences.

*Public Sector*

It is difficult to estimate the impact of the removal of the £10 fee on the wider public sector, because the number of SARs varies greatly from department to department. For example, whereas the UK Border Agency (UKBA) receives around 22,700 SARs a year, the Department for Work and Pensions receives between 7,000 and 10,000 a year, and the central part of the Department for Transport receives between 25 and 50 a year<sup>26</sup>.

While it is therefore not possible to estimate the cost for the whole Public Sector, the impact on departments processing large numbers of SARs can be illustrated by the example of UKBA. UKBA currently receive over 22,000 SARs a year and an increase of 25-40% would cost in the region of an additional £1m annually to process.

**Data Protection Impact Assessments (DPIAs)**

Article 33 specifies that a data protection impact assessment (DPIA) must be carried out when “operations present specific risks to the rights and freedoms of data subjects”. These circumstances are particularised in article 33(2) and include *inter alia* profiling, processing of sensitive types of personal data, monitoring of publicly accessible areas (for example, using CCTV) and the use of large scale filing systems with children’s data, genetic data or biometric data. While it is unclear exactly which data controllers will be captured by this article as it is currently worded, Annex A gives a list of 42,000 SME and micro businesses that may be expected to carry out DPIAs based upon their business classification. This list is likely to under-estimate the number of SMEs needing to do DPIAs, however, in particular as many controllers will undertake CCTV monitoring. It is expected that all large data controllers would have to carry out DPIAs, given they will be processing large amounts of personal data – this gives 4,500 large organisations that would need to carry out DPIAs.

<sup>26</sup> Based on response to the Post Implementation Review of the Data Protection Act; SARs to the Department for Transport excludes requests to DVLA, DSA, VOSA and the Highways Agency.

The proposed Regulation is very prescriptive as to what the DPIA must include. For example, it specifies that the controller must seek the views of data subjects which is expected to be a particularly costly part of the process. The EU Commission estimate that carrying out a DPIA could cost the following<sup>27</sup>:

Small scale DPIA:	€14,000 (£11,200)
Medium scale DPIA:	€34,500 (£27,600)
Large scale DPIA:	€149,000 (£119,200)

However, the large scale DPIA is an extreme example of a large project involving sensitive data and so it is not used in this assessment.

## Benefits

The ICO Handbook states<sup>28</sup>:

*“By performing a Privacy Impact Assessment early in a project, an organisation avoids problems being discovered at a later stage, when the costs of making significant changes will be much greater.”*

Indeed, studies carried out into Privacy Impact Assessments conclude that they benefit organisations because they enable privacy risks to be identified prior to programmes being put in place<sup>29</sup>.

The monetary benefits of performing a DPIA have been included in the reduction in data breaches, estimated above.

## Costs

As the ICO already encourages organisations to carry out PIAs, a significant number of organisations will be doing these already. For example, Microsoft alone undertakes 2,000 PIAs a year. As a proxy for the number of private sector organisations already carrying out DPIAs, data from a PWC survey on the number of organisations carrying out information security risk assessments has been used; although, there may still be additional costs for those already carrying out PIAs due to the need to consult data subjects which cannot be factored in here. This is shown in Table 4.9<sup>30</sup>.

**Table 4.9: Number of data controllers carrying out DPIAs**

Business by size	Number of Affected Controllers	% that don't carry out security risk assessments	Increase in controllers doing DPIAs
Micro	23,730	26%	6,170
SME	18,405	26%	4,785
Large	4,500	11%	495
<b>Total</b>	<b>46,635</b>		<b>11,450</b>

Note: numbers may not sum due to rounding.

Based on the EU Commission estimates above, the cost of a DPIA will be £27,600 for a large organisation and £11,200 for a small organisation (on the assumption that the scale of the assessment equates to the scale of the organisation). Large DPIAs, costing £119,200, are not included since this estimate is only for large projects involving very risky processing.

It is expected that medium and large controllers will need to do at least one DPIA each year; however, this is less likely to be the case for micro businesses and so for this reason a range is given to show that micro businesses may not need to carry out DPIAs at all. The unit cost for micro organisations has also been divided by five to reflect that micro organisations would be unlikely to do more than one impact

<sup>27</sup> EU Commission Impact Assessment

<sup>28</sup> ICO (2012). Privacy Impact Assessment Handbook. [http://www.ico.gov.uk/upload/documents/pia\\_handbook\\_html\\_v2/](http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/)

<sup>29</sup> Linden Consulting (2007), 'Privacy Impact Assessments: International Study of their Application and Effects'.

<sup>30</sup> PWC (2012), Information security breaches survey: technical report.

assessment in a five year period. Table 4.10 estimates the additional cost to business of the DPIA requirement. It is estimated that carrying out a DPIA will cost business between £67 and £81 million per annum in 2012-13 earnings terms. The range reflects the uncertainty in whether micro organisations processing risky data will be required to carry out DPIAs. These estimates can be considered conservative since it is likely that larger organisations will need to carry out more than one assessment a year.

**Table 4.10: Annual cost of carrying out DPIAs (£millions; 2012-13 earnings terms)**

	Unit Cost Low	Unit Cost High	Number of firms	Total Cost Low (£millions)	Total Cost high (£million)
<b>Micro</b>	£0	£2,240	6,170	£0	£14
<b>SME</b>	£11,200	£11,200	4,785	£54	£54
<b>Large</b>	£27,600	£27,600	495	£14	£14
<b>Total</b>				<b>£67</b>	<b>£81</b>

### *Public Sector*

The Data Handling Procedures in Government Report (informally known as the Hannigan Review) mandated all government departments to use Privacy Impact Assessments from July 2008 and so these should already be being carried out across central government<sup>31</sup>. However, there has been no government-wide monitoring of how many PIAs are carried out annually.

### Data Protection Officers (DPOs)

Article 35 of the proposed Regulation states that a DPO must be designated where the processing is carried out by a public authority, the processing is carried out by a business employing 250 people or more, or the core activities of the controller or the processor require regular and systematic monitoring of data subjects. Annex A sets out a list of micro and SMEs that are likely to be caught by the DPO requirement.

### *Benefits*

If employing a DPO enables an organisation to implement a proactive policy on data security then this part of the Regulation may help to reduce the loss and theft of personal data, as captured in the 'reduction in loss of personal data' saving. However, it is not necessarily the case that the detail set out in the Regulation as to what a data controller must do will directly lead to any benefits for the organisation.

### *Costs*

The EU Commission estimates that 10% of organisations will need to employ a DPO costing €80,000 per annum (£64,000)<sup>32</sup>. The ICO estimates that a vast majority of large organisations typically have a team responsible for data protection, and so costs depend on how easily one person can be appointed to this role. Assuming that most large organisations can appoint a person already responsible for data protection as the DPO, then the assumption that 10% of large organisations will need to recruit a DPO seems reasonable. This assumption has been extended to the public sector.

The CBI estimate that a DPO can cost between £30,000 and £75,000 per annum<sup>33</sup>. BIS Business Population Estimates for 2011 find that there are 6,320 businesses and 1,490 central and local government employers employing 250 people or more. Assuming that 10% of these organisations need to employ a DPO, this gives an additional cost of £19-£47 million p.a. in 2012-13 earnings terms for the

<sup>31</sup> Details of the Hannigan Review can be found here: <http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf>, accessed: 19/11/2012.

<sup>32</sup> EU Commission Impact Assessment. Annex 6, page 120.

<sup>33</sup> CBI response to the UK Call for Evidence on the data protection proposals. Published here [http://www.cbi.org.uk/media/1356711/cbi\\_response\\_\\_data\\_protection\\_in\\_the\\_eu\\_\\_feb\\_2012\\_.pdf](http://www.cbi.org.uk/media/1356711/cbi_response__data_protection_in_the_eu__feb_2012_.pdf)

private sector and £4-£11 million p.a. in 2013-13 earnings terms for the public sector based on the salary range for a DPO.

However, the Regulation does set out strict criteria for the qualifications and tasks of the DPO. For example, the DPO must be designated for a minimum of two years, must have expert knowledge of data protection law, and carry out tasks and duties 'independently'. Organisations that appoint an existing member of staff to this role may therefore still incur costs if they have to retrain this staff member and provide them with a new contract of employment.

There are approximately 42,000 SMEs and micro businesses that would be expected to designate a DPO based on the assessment given in Annex A. The EU Commission estimates that SMEs and micro businesses can fulfil the requirements of the Regulation by employing four hours of legal validation work per annum costing €1,000 (£800). This is a cost of £34 million in 2012-13.

However, while four hours of legal work may be sufficient for micro businesses it is unlikely to be sufficient to fulfil the requirements of the Regulation for medium-sized businesses. Of the organisations listed in Annex A, nearly 3,000 are medium sized businesses. If these organisations appoint a full-time DPO then this brings the total cost to SMEs to £182 million. Therefore, the cost of designating a DPO for SMEs and micro businesses is in the range of £34-£182 million p.a. in 2012-13 earnings terms.

There are 3,600 public sector organisations employing fewer than 250 people that would also be expected to appoint a DPO<sup>34</sup>. Assuming that each one of these requires four hours of legal validation work, this is a cost of £3 million p.a. in 2012-13 earnings terms.

Table 4.11 summarises the annual cost of employing a data protection officer. The salary of a DPO is expected to grow in line with forecast earnings growth.

**Table 4.11: Annual Cost of employing Data Protection Officers; £millions, 2012-13 earnings terms.**

	<b>Low</b>	<b>Mid/Best</b>	<b>High</b>
Private Large	£19	£33	£47
Public Large	£4	£8	£11
Private small	£34	£108	£182
Public Small	£3	£3	£3
<b>Total</b>	<b>£60</b>	<b>£152</b>	<b>£244</b>

#### Information Commissioner's Office (ICO)

The Regulation imposes new burdens on the supervisory authority both because it increases the burden on activities that the ICO currently does, but also because it introduces new functions for the supervisory authority. These additional burdens (as estimated by the ICO) are set out below:

#### Increased burdens:

- The requirement to notify data breaches to the supervisory authority will increase the number of data protection breaches that the ICO has to investigate.
- The requirement to have either a contractual clause or binding corporate rule in place before transferring personal data outside the EEA will increase the number of binding corporate rules that the ICO has to approve.
- There is likely to be an increase in the use of administrative sanctions which will place an additional burden on the ICO, particularly as the ICO has less discretion on whether to take formal action.
- The ICO expect that the Regulation will increase the current cost of providing support for data controllers
- The ICO also expects an increase in data protection complaints as a result of the Regulation, particularly from the 'right to be forgotten'.

<sup>34</sup> BIS Business Population Estimates 2011.

- Representing the UK at a European level – participation in the consistency mechanism work is expected to be particularly onerous.

#### New burdens:

- Article 34 would require the supervisory authority to give prior authorisation to controllers and processors where they use non-standard contractual clauses and appropriate safeguards outside a legally binding instrument for international data transfers. There are also extensive prior consultation requirements under Article 34 for risky or other specified types of processing.
- Article 74 would give each individual the right to a judicial remedy against the supervisory authority, leading to an increase in legal costs for the ICO.

As noted above, the ICO will also lose its notification fee income, estimated at £15.6 million in 2012-13.

#### *Benefit*

Administering the notification fee does have a cost to the ICO through staff and support costs and so there will be a saving from no longer being able to charge a notification fee. This is estimated by the ICO to be a saving of £750,000 in 2012-13 which will grow in line with earnings.

#### *Cost*

The ICO estimates that the additional duties of the Regulation will cost the organisation an additional £8-£26 million per annum in staff costs. There will also be an additional £0.4-£1.7 million in support costs. The breakdown for these costs (estimated by the ICO) is given in table 4.12.

Added to this cost is the loss of notification fee income (minus the saving from no longer having to administer the notification fee). This gives a total cost to the ICO of between £24 and £44 million per annum, and a net cost of £23-£43 million when the benefit from not having to collect the notification fee is included. These costs are assumed to grow in line with earnings. These additional costs compare to a total spend on data protection work of £16 million in 2011-12<sup>35</sup>.

**Table 4.12: additional cost to the ICO (£millions; 2012-13 estimates).**

	<b>Lowest Projection</b>	<b>Realistic Projection</b>
<b>Staff Costs</b>		
Prior Authorisation	£0.5	£3.0
Binding Corporate Rules	£3.3	£6.5
Prior Consultation	£0.3	£0.5
Breach notification	£2.8	£7.0
Administrative sanctions	£0.2	£8.3
European involvement	£0.2	£0.2
Complaints	£0.2	£0.5
Judicial reviews	£0.6	£0.4
<b>Total staff costs</b>	<b>£8.0</b>	<b>£26.3</b>
Support Service	£0.4	£1.7
<b>Total Cost</b>	<b>£8.4</b>	<b>£28.0</b>
<b>Plus loss of notification fee</b>	<b>£24.0</b>	<b>£43.6</b>
<b>Plus gain from not collecting notification fee</b>	<b>£23.3</b>	<b>£42.8</b>

<sup>35</sup> ICO (2012), Information Commissioner's Annual Report and Financial Statements 2011/12.



## **5. Direct costs and benefits to business calculation (following OIOO methodology)**

The Regulation would result in both benefits and costs to business, as detailed above. However, as the total costs outweigh the total benefits the Regulation is expected to result in a net 'in' to business.

Following the OIOO methodology the Equivalent Annual Net Cost to Business (EANCB) has been calculated using a 14 year appraisal period and a discount rate of 3.5%. The costs to business have been deflated into 2009 prices and discounted to 2010-11. Using this methodology gives a benefit to business of £100 million and a cost to business of £230 million, giving an EANCB figure of -£130 million. However, the Regulation is out of scope for OIOO because it is an EU measure.

## **6. Non-monetised Costs and Benefits**

The Regulation has a number of costs and benefits which it is not possible to quantify with the evidence available to us. Two non-monetised benefits are identified in this section:

- enhanced control for data subjects over their personal data, which will be achieved through the 'right to be forgotten', data portability and the strengthening of rights of access and rectification;
- a reduction in identity theft achieved through enhanced security protection.

Data portability is also expected to lead to economic benefits by lowering prices and increasing competition for services, in line with the Government's midata initiative<sup>36</sup>.

However, the Regulation also introduces further costs which are not possible to quantify. While data portability and the 'right to be forgotten' are beneficial for individuals, both are expected to be costly to data controllers to implement. Indeed, many controllers think the 'right to be forgotten' could be impossible to implement due to the way data is copied rapidly across the internet, leading to consumer expectations not being met. The Regulation also introduces higher standards for consent, and profiling which could be costly for data controllers, and gives data controllers less flexibility when transferring data outside of the EEA. The changes to consent and profiling, along with uncertainty around the definition of personal data, are likely to be particularly costly for the advertising sector whose business model could be impacted by these measures and is likely to have knock-on impacts to growth in the internet economy.

The administrative sanctions set out in the Regulation are also a cost to business since they are disproportionate to the harm caused. Such high fines are expected to lead to data controllers spending a disproportionate amount of resource to ensure technical compliance with data protection legislation.

### **Enhanced protection of personal data**

The section on monetised costs and benefits showed that by implementing a number of different aspects of the Regulation, organisations should see a reduction in the amount of personal data that is lost or obtained fraudulently. The benefit to business of a reduction in data breaches was estimated to be between £58 million and £124 million per annum in 2012-13 earnings terms. However, there is also likely to be some additional benefit to data subjects if this reduces the amount of personal data that is obtained and used fraudulently.

A 2009 survey estimated that in the course of a year 12% of UK citizens had been victims of online ID fraud, with an average financial loss per victim of £463<sup>37</sup>. A quarter of victims surveyed were still in dispute over compensation for the money that was stolen from them. It is not possible to quantify the reduction in identity fraud that could result from the Regulation being implemented, but if companies succeed in reducing the amount of personal data that is lost – as quantified in the previous section – this should have knock-on benefits for individuals whose data may have otherwise been used fraudulently.

<sup>36</sup> See <http://www.bis.gov.uk/policies/consumer-issues/consumer-empowerment/personal-data>.

<sup>37</sup> One in Eight Fall Victim to Online ID Fraud. Press Release about YouGov survey, Verisign 16 September 2009. [http://www.symantec.com/about/news/release/article.jsp?prid=20090916\\_02&company=verisign](http://www.symantec.com/about/news/release/article.jsp?prid=20090916_02&company=verisign)

There are also likely to be increased economic benefits if, as a result of the increased protection of personal data, individuals are more willing to use services that require them to share their personal data. For example, a survey carried out by Populus found that 76% of individuals in the UK were worried about companies losing their personal data, while a 2009 survey by Eurostat found that privacy and trust concerns were amongst the top reasons that EU citizens chose not to shop online<sup>38</sup>. There is therefore scope to increase consumer confidence, and economic growth, by enabling consumers to feel more confident sharing their personal data online.

## Right to be Forgotten

The Regulation also gives individuals greater control over the personal data that is held about them. Article 17 gives individuals a 'right to be forgotten' meaning that the data subject has the right to request that the controller erase all personal data held about them and where the controller has made the personal data public can require the fact of deletion to be passed onto third parties to whom the data has been disclosed. Under the current Data Protection Act (DPA) a court can require that personal data be erased if it is inaccurate or is causing a data subject damage, and a court can require the fact of deletion to be passed on to third parties to whom the data has been disclosed. The Regulation therefore strengthens the existing 'right to erasure' and widens the scope under which it can be used.

In a recent survey carried out by the EU Commission 16% of UK individuals questioned said they felt they had "no control" over information they had disclosed on social networking sites and 51% felt they had only "partial control"<sup>39</sup>. This suggests that individuals will benefit from being given strengthened rights to erase and rectify personal data that is held about them. In a survey carried out by Populus, 73% of individuals said 'the ability to withdraw my data' would make them more comfortable with sharing information. This suggests that the 'right to be forgotten' could generate growth in the internet economy if consumers are more willing to use services that require them to share their personal data<sup>40</sup>.

However, a number of data controllers have expressed concern about the practicalities of being able to implement a 'right to be forgotten' in an age where digital data is replicated across the internet. Microsoft is just one controller that argues that it will be impossible to erase all traces of someone's personal data because digital data is often quickly replicated across the web with no contractual relationship in place<sup>41</sup>. Therefore, it is not clear whether the benefit of this proposal will materialise. A number of businesses have also expressed concern that this would weaken consumer trust in their organisation if they cannot deliver a right which consumers have been told to expect.

Some businesses have expressed concern that the 'right to be forgotten' could be costly to implement due to the need to update record keeping systems in order to be compliant, although this view is not shared across all organisations. Evidence from the CBI found that some businesses expect there to be significant costs through audit and record keeping, while others suggest that records of data erasure are already kept and so would not be an additional burden<sup>42</sup>. In response to the UK Call for Evidence some businesses provided estimates of the cost of updating their IT systems to be compliant with the 'right to be forgotten' and data portability. These estimates are given below in the section on data portability.

## Data Portability

Article 18 of the Regulation states that a data subject will have the right to obtain from the controller:

- A copy of any data undergoing processing in an electronic form that allows for further re-use;
- A right to share that data with another controller;
- The data in an electronic form specified by the EU Commission.

---

<sup>38</sup> Bartlett, Jamie (2012), 'The Data Dialogue', published by Demos ;EU Commission Impact Assessment, pages 26-27;

<sup>39</sup> EU Commission (2011), 'Attitudes on data protection and electronic identity in the European Union'. Special Eurobarometer 359.

<sup>40</sup> Bartlett, Jamie (2012), 'The Data Dialogue', published by Demos.

<sup>41</sup> Microsoft response to MOJ Call for Evidence (2012).

<sup>42</sup> Evidence provided by the Confederation of Business Industry in discussion with businesses.

The Department for Business and Skills (BIS) has already proposed introducing something similar to this right through its midata initiative. A BIS consultation on the proposals closed in September 2011, the details of which can be found on the BIS website<sup>43</sup>. Midata, and similar schemes run proactively by organisations are already in place, but the BIS consultation explores the possibility of taking a power to make it legally enforceable on a sector by sector basis. The additional costs and benefits of data portability as set out in the Regulation will therefore depend on the extent to which the midata proposals are legally enforceable, the extent to which organisations proactively offer such services, and the take from consumers at the time when the Regulation is introduced.

### *Benefits*

Data portability is a benefit to the consumer because it enables them to seek the lowest price for a good by accessing all of their information. For example, in the mobile phone market if the consumer cannot accurately measure how much they use their mobile phone then they may remain on a tariff that is unsuitable for them, even though by shopping around they may be able to find a tariff that gives them the same usage but for a lower cost. By being able to access all of their phone usage data, consumers can more easily force firms to compete to offer them the best price. This in turn leads to increased competition and the development of new products, as well as intermediary firms being set up to enable consumers to use their data to search for the best tariff.

It is difficult to measure the economic benefit that data portability will bring because it depends on the consumer making use of their data. However, estimates are available for certain markets on the money that consumers are missing out on by being on a contract that is costing more than a more suitable alternative:

- Billmonitor found being on the wrong mobile phone contract cost UK citizens £5.98 billion in 2011<sup>44</sup>.
- through the Big Switch, an initiative run by the consumer and rights groups Which? and 38 Degrees, approximately 200,000 households could have saved £123 a year, a total saving of £25 million a year<sup>45</sup>.

These savings are available now, but due to the effort required by consumers to investigate these savings they are not realised. The gain from data portability will therefore depend on the extent to which data portability reduces the cost to consumers of researching better deals and tariffs and the extent to which consumers make use of this new right.

### *Cost*

In response to the 2012 Call for Evidence businesses cited data portability as a costly part of the Regulation due to the need to modify existing technology in order to comply with the requirement to provide data subjects with their data in a specific electronic format. Even with midata there could still be costs to business if the EU Commission specifies a format different from that the business already uses.

The CBI discussed the possible costs of data portability with a number of businesses. One mid-sized digital marketing agency stated that set up costs were likely to be “thousands” but would vary depending on complexity and the number of data feeds involved. In response to the Call for Evidence a number of organisations cited specific costs from new system development to comply with both data portability and the right to be forgotten:

- A member of the Direct Marketing Association (UK) estimated that the data portability and ‘right to be forgotten’ clauses could require a one-off system development costing £100,000;
- A large telecommunications business estimated that data protection by design, data portability and the right to be forgotten would cost £5 million in system development.

---

<sup>43</sup> <http://www.bis.gov.uk/assets/biscore/consumer-issues/docs/m/12-943-midata-2012-review-and-consultation.pdf>. Accessed: 02/11/2012.

<sup>44</sup> Bill monitor (2012), ‘The bill monitor.com national mobile phone report 2012’.

<sup>45</sup> <http://www.myfamilyclub.co.uk/news/which-big-switch-to-save-families-123-a-year-15235>

It is difficult to extract from these figures the exact cost of complying with data portability, since setting up new IT systems to comply with the Regulation is likely to be caught up with other measures, such as the right to be forgotten. Costs are also likely to vary for different sized organisations.

There is also concern about the impact this could have on an organisation's ability to protect their intellectual property. For example, one large advertising company expressed concern that an individual could request all of their data collected in panel surveys and then sell it to a rival company<sup>46</sup>.

The number of data controllers affected by data portability has been estimated using BIS Population estimates. As data portability is designed to allow individuals to transfer their data to another service provider it has been assumed that private organisations where information is required for service provision are affected. The organisations affected are assumed to be:

- energy suppliers
- large retailers
- telecommunications providers;
- information services;
- financial services.

Table 6.1 shows the number of affected organisations, split by firm size and service type. It is assumed that micro organisations are not affected by data portability and that for retail only very large employers are affected. Table 6.1 shows that there are around 1,700 firms that could be affected by data portability.

**Table 6.1: Organisations affected by data portability**

	<b>Electricity, gas, steam and air conditioning supply</b>	<b>Retail Trade</b>	<b>Telecommunic ations</b>	<b>Information Service activities</b>	<b>Financial Services</b>	<b>Total</b>
1-19	Excluded	Excluded	Excluded	Excluded	Excluded	
20-49	40	Excluded	235	145	Excluded	420
50-99	25	Excluded	80	40	195	340
100-199	15	Excluded	35	25	115	190
200-249	0	Excluded	10	5	15	30
249-499	5	180	20	10	50	265
500+	20	300	25	10	115	470
<b>Total</b>	<b>105</b>	<b>480</b>	<b>405</b>	<b>235</b>	<b>490</b>	<b>1,715</b>

Source: BIS Business population estimates 2011

### Administrative sanctions

Article 79 sets out the administrative sanctions for failure to comply with the Regulation. The article proposes a three tier fine system:

- Tier 1: €250,000 / 0.5% annual worldwide turnover for business
- Tier 2: €500,000 / 1% annual worldwide turnover for business
- Tier 3: €1,000,000 / 2% annual worldwide turnover for business

The maximum financial penalties set out in the Regulation are arguably more severe than the current ICO monetary penalties, with a requirement that high financial penalties be imposed for less serious breaches of data protection law than is currently the case. For example, a tier 1 fine can be imposed for failure to comply with a SAR, a tier 2 fine can be imposed for failure to maintain the correct documentation, and a tier 3 fine can be imposed if a firm does not designate a DPO. Financial penalties

<sup>46</sup> Evidence provided by the Confederation of Business Industry in discussion with businesses.

are imposed in these situations regardless of the harm caused, although a warning may be given for a non-intentional first offence committed by an organisation employing less than 250 people.

Under the current DPA the ICO can issue a monetary penalty up to £500,000 for the most serious breaches of the Act's principles which has caused, or could have caused, serious damage or serious distress to individuals. In 2011/12 ten monetary penalties were issued totalling £1,171,000<sup>47</sup>. However, as drafted, the proposal does not give discretion to the Information Commissioner not to fine when he is satisfied that there has been a breach of the Regulation's requirements. We may therefore expect more fines to be handed down in future, particularly for the lower level, non-harm based breaches set out in article 79.

If the fine regime set out in the Regulation were imposed in all cases where data controllers are found to be non-compliant then the cost to a business and the public sector would be considerable. For the Information and Communication sector, average turnover for SMEs and large organisations in 2011 was £18 million, but when micros are included the average turnover is £3 million - this gives the following average fine maximums, depending on whether micros are included<sup>48</sup>:

- Tier 1 (0.05% of turnover): £15,000 - £90,000
- Tier 2 (0.1% of turnover): £30,000 - £179,000
- Tier 3 (0.2% of turnover): £60,000 - £359,000.

According to economic theory, an optimal fine should be set so that the cost of committing an offence outweighs the benefit<sup>49</sup>. Thus the optimal fine should be set where the fine multiplied by the probability of getting caught is greater than the cost of complying with data protection legislation. However, fines should not be set so high that they incentivise data controllers to spend more than is necessary on data protection at the expense of other areas. For example, if a firm has to decide how to spend a limited pool of resource to ensure it is compliant with several areas of legislation, such as a data protection and health and safety, it is likely to focus spending on the area(s) with the largest financial penalty. Fines that are disproportionate to the harm caused are therefore bad for businesses since they lead to mis-allocation of administrative spending.

The fines set out in the data protection Regulation are considered to excessive compared to the harm caused. For example, charging a fee for a SAR attracts a tier 1 fine (0.05% of turnover), while not providing data in an electronic format attracts a tier 2 fine (0.1% of turnover). Fines of this magnitude are likely to lead to data controllers spending more than is necessary on legal consultants to ensure they are compliant with data protection legislation.

Additionally, in extreme cases such a high fine could force a marginal firm out of business. For example, if a business is already struggling financially, and therefore finding it difficult to comply with the Regulation, imposing a fine of this magnitude could be extremely damaging for the business. The Federation of Small Business raised this concern in response the Call for Evidence, stating that "some of the fines envisaged in the proposal will be significant sums of money to a small business, forcing some of them to close".

### International Transfers

In the UK the Information Commissioner offers guidance to organisations about how they may comply with the DPA's requirements about personal data transfers to non-EEA countries, but takes the view that responsibility for ensuring the proposed transfer of personal data to such countries rests with the data controller. Under the Regulation to transfer data to a non-EEA country the controller will need either:

- a) an adequacy decision from the Commission (article 41); or
- b) adequate safeguards to be put in place, such as binding corporate rules or contractual clauses. These will require prior approval from the supervisory authority (article 43)

---

<sup>47</sup> Information Commissioner's Office (2012), Information Commissioner's Annual Report and Financial Statements 2011/12.

<sup>48</sup> BIS Population Estimates 2011.

<sup>49</sup> London Economics (2009), An assessment of discretionary penalties regimes, Published by the Office of Fair Trading.

There are a number of derogations set out in article 44 which organisations may be able to rely on to make transfers. However, unless data controllers can rely on the derogations, seeking approval from the supervisory authority will increase the cost to business of transferring data outside of the EEA. There may also be additional legal costs if organisations need advice on whether the derogations apply.

A survey of companies employing at least 20 people carried out in 2008 asked organisations whether they transferred personal data outside of the EU<sup>50</sup>. 11.1% of UK companies surveyed said that they did transfer personal data outside of the EU, compared to 9.5% of organisations across the 27 EU Member States. Business Population Estimates show that in 2011 there were 100,465 private sector organisations in the UK employing at least 20 people. This equates to around 11,000 organisations that could be affected by the new rules on international transfers.

As the UK supervisory authority has only approved 15 Binding Corporate Rules so far, the Regulation is likely to be costly for business and for the UK supervisory authority. The process of achieving approval for binding corporate rules currently takes around 9 months to a year from receipt of the first draft.

### Profiling, consent, and definition of personal data

Article 20 forbids “automated processing of personal data intended to evaluate certain personal aspects”, while article 4 amends the definition of personal data to include online identifiers and requires that consent must be “specific, informed and explicit”. The requirement for consent to be “explicit” goes further than the current Directive and DPA. In response to the UK’s recent Call for Evidence over half of respondents felt that this would require controllers to give data subjects an “opt-in” for their personal data to be collected, where this is the legal basis being relied upon. When read together with the revised e-Privacy Directive’s requirement that the user’s consent be gained when storing or accessing information on a user’s terminal equipment, these articles are likely to be extremely detrimental to growth in the technology sector, due to the restrictions they place on direct marketing.

### Cost

The direct marketing industry identifies specific characteristics about consumers in order to produce personalised adverts, while advertising agencies use this information to tailor adverts to their receivers. DMA (UK) estimate that in 2011 £14.2 billion was spent in the UK on direct marketing; restrictions in this market are therefore likely to be costly to the UK economy<sup>51</sup>. The Internet Advertising Bureau estimates that the proposals as drafted may cost the UK an estimated £633 million in lost advertising revenues as companies reduce their advertising expenditure, while the effect on businesses overall was estimated by DMA (UK) to be £47 billion, due to the inability to target consumers directly<sup>52</sup>.

These articles may also restrict growth in the internet economy due to the limitations they place on web-based advertising. Web services, such as search engines, are able to be provided free of charge because they generate revenue through personalised advertising. If less money were spent on advertising and the adverts were less effective it would reduce the extent to which advertising companies would subsidise such services, which would be detrimental to the end user.

There could also be a cost to the IT sector through a reduction in investment in internet start-ups. In 2012 Booz&co. carried out a survey with 189 angel investors and 24 venture capitalists to understand the impact that changes in privacy regulations could have on their decision to invest in advertising technology companies. While the survey was for the US, angel investors and venture capitalists invested nearly €3.8 billion in Europe in 2010 (around half of which was in the high-tech sector) and so the survey results are relevant to Europe<sup>53</sup>.

---

<sup>50</sup> EU Commission (2008), ‘Data protection in the European Union: data controller’s perceptions’. Flash Barometer 226.

<sup>51</sup> DMA (2012), ‘Putting a price on direct marketing’.

<sup>52</sup> DMA (2012), ‘Putting a price on direct marketing’. The £47 billion figure was calculated from a survey of 600 UK companies who were asked how their businesses would respond if they could no longer use web analytics for marketing purposes. This includes the loss to advertising companies.

<sup>53</sup> Le Merle et al (2012), ‘The impact of US internet privacy regulations on early-stage investment. A quantitative study.’ Booz&co.

The survey by booz&co. found that privacy regulations requiring opt-in before any data is collected would reduce the pool of interested investors in advertising technology companies by 65%<sup>54</sup>. This suggests that the rules around consent could have a negative impact on investment in the internet industry. However, such a survey question is likely to trigger a negative response, and so if consent is not too costly to obtain under the Regulation the impact on investment may not be as detrimental as this survey suggests.

Finally, the requirement for consent to be explicit may limit the ability of certain organisations to develop new products that rely on personal data<sup>55</sup>. This may particularly be the case for new products which rely on locational data and information about a user's preferences.

### *Benefit*

However, placing restrictions on personalised advertising will be beneficial to the consumer if it limits price discrimination. As companies possess more information they have a greater ability to price discriminate, i.e. offer personalised prices based on their information about the consumer's budget and spending habits. Placing restrictions on behavioural advertising therefore limits the ability of businesses to charge higher prices by targeting those customers with a higher marginal willingness to pay.

The requirement to obtain explicit consent may also be seen as a benefit to many consumers who will no longer receive marketing which they do not want and will be more confident about sharing their data online. The restrictions that the Regulation places on personalised advertising should lead to a culture where direct marketing is focused on those who have requested it, preventing consumers being presented with marketing which they do not want.

---

<sup>54</sup> Le Merle et al (2012), 'The impact of US internet privacy regulations on early-stage investment. A quantitative study.' Booz&co.

<sup>55</sup> Information Technology and Innovation Foundation response to the MOJ Call for Evidence.

## Annexes

### Annex A: Underlying data

#### *Economic Assumptions*

The headline figures are shown in 2012 prices. The GDP deflator has been used to convert figures into 2012 prices.

Office for Budget Responsibility (OBR) projections of average earnings growth have been used to up rate the cost of staff activities. The OBR March 2012 projections have been used for 2013 through to 2016. For 2017 onwards, the OBR long-term projection of average earnings growth of 4.75% has been used.

Figures in euros have been converted to GBP using an exchange rate of £1=€1.25.

#### *Business Population Estimates*

The 2011 Business Population Estimates published by BIS have been used as an input source for much of the monetised cost/benefit analysis. These are published here (<http://www.bis.gov.uk/analysis/statistics/business-population-estimates>).

#### *Number of data controllers*

According to the ICO website, 355,000 organisations notify as data controllers<sup>56</sup>. This is an estimate of the number of organisations affected by the Regulation in the UK, although it will exclude controllers exempt from notification.

Data controllers exempt from notifying are as follows:

1. Data controllers who only process personal information for staff administration, advertising, marketing and publication in connection with their own business activity, and accounts and records.
2. Some non-for-profit organisations.
3. Processing personal information for personal, family or household affairs.
4. Processing personal information without an automated system, such as a computer.

#### Split by size of organisation

Since 2010/11 the ICO has had a two tier notification fee system. There is a £500 fee for public sector organisations employing at least 250 people and for private sector organisations employing 250 people with an annual turnover of at least £25.9 million. All other organisations pay a fee of £35.

The ICO does not report on exactly how many organisations pay the higher and lower tier fee and so this has been approximated using income received from the two different fee tiers, given in table A.1. To calculate the number of organisations paying the higher and lower fee, an average has been taken for 2010-11 and 2011-12 and rounded to the nearest 1,000. This gives approximately 6,000 organisations paying the higher tier fee and 349,000 organisations paying the lower fee – giving a total of 355,000 data controllers.

---

<sup>56</sup> [http://www.ico.gov.uk/about\\_us/our\\_organisation/key\\_facts.aspx](http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx). Accessed: 02/11/2012.



**Table A.1: Income received under different fee tiers, and approximate number of organisations registering with the ICO**

	<b>Tier 1 Income</b>	<b>Tier 1 Organisations</b>	<b>Tier 2 Income</b>	<b>Tier 2 Organisations</b>
<b>2010-11</b>	£11,913,172	340,376	£2,961,100	5,922
<b>2011-12</b>	£12,549,176	358,548	£2,801,952	5,604
<b>Average</b>		349,000		6,000

Source: ICO website ([http://www.ico.gov.uk/about\\_us/our\\_spending.aspx](http://www.ico.gov.uk/about_us/our_spending.aspx)). The 'average' has been rounded to the nearest 1,000.

#### Public/Private Split

The ICO does not report the public/private split of the organisations registered with it. However, a piece of research carried out in March 2008 reported the proportion of private organisations registered with the ICO to be 54%. This was based on a random sample of 1,100 organisations taken from the public register – enough to ensure a confidence level of 95%<sup>57</sup>. If 54% of data controllers are private sector organisations, this gives a total of 191,700 private sector data controllers.

However, it is likely that the proportion of large organisations registered with the data controller is greater than 54%. According to the Business Population Estimates for 2011 there were 6,320 private sector organisations and 1,490 public sector organisations employing at least 250 people. It is reasonable to assume that all large public organisations are registered with the data controller, leaving approximately 4,500 large private sector organisations (75%) paying the higher fee.

If there are 191,700 private sector data controllers and 4,500 of them are large organisations, this leaves 187,200 small private sector businesses that are data controllers.

#### ***SMEs affected by the Regulation***

There are particular aspects of the Regulation that only affect businesses employing fewer than 250 people if their processing requires regular and systematic monitoring of data subjects. This is particularly relevant for the requirements on DPOs, DPIAs and documentation.

Using the 2011 Business Population Estimates a list of businesses that could fall into this category has been drawn up. This is shown in Table A.2. There are 64,475 businesses in total that fall into this category. However, if micro organisations are excluded the number falls to 18,405. It is difficult to know whether to include or exclude micro business from this list and so has a judgement has been made according to whether a particular type of micro organisation might be expected to carry out regular and systematic monitoring of data subjects. The final list is given in the third column and shows that there are just over 42,000 SMEs and micro businesses who's processing would require them to employ a DPO, conduct DPIAs and document all processing.

<sup>57</sup> Social and Market Strategic Research (2008), 'Notifications payment consultation'.

**Table A.2: SMEs and micro businesses, split by Business group, who could be classified as carrying out regular and systematic processing of data subjects**

	<b>SME and Micro</b>	<b>Just SMEs</b>	<b>Businesses carrying out regular and systematic monitoring of data subjects</b>
Data processing, hosting and related activities; web portals	1,560	310	1,560
Other information service activities	1,280	135	1,280
Trusts, funds and similar entities	540	130	130
Other financial service activities, except insurance and pension funding	3,745	575	575
Insurance	1,020	260	1,020
Reinsurance	15	10	10
Pension funding	0	0	0
Advertising	6,685	1,195	1,195
Market research and public opinion polling	1,550	385	1,550
Private security activities	3,135	1,000	3,135
security systems activities	730	100	730
Investigation activities	205	20	205
Hospital activities	1,470	1,085	1,470
Medical and dental practice activities	24,555	8,480	24,555
Other human health activities	7,135	890	890
Wired telecommunication activities	215	50	50
Wireless telecommunication activities	235	55	55
Satellite communication activities	45	10	10
Other telecommunication activities	2,250	525	525
Temporary employment agency	8,105	3,190	3,190
<b>Total:</b>	<b>64,475</b>	<b>18,405</b>	<b>42,135</b>

Source: BIS Business Population Estimates, 2011

## Evidence from the CBI

The Confederation of British Industry (CBI) spoke with a number of businesses about the costs of data portability, the 'right to be forgotten', international transfers and data protection officers. They received responses from a large Bank, a large advertising agency, a mid-cap digital marketing agency, a large digital marketing agency and a regional legal firm. Their responses are used throughout the impact assessment, particularly in the section on non-monetised costs and benefits.

## **Annex B**

### **Specific impact tests**

#### **Impact on Small Businesses**

##### **Summary**

Small businesses are less likely to be affected by legal fragmentation than large multinational organisations since they are less likely to be established across multiple Member States. The benefit of a harmonised Regulation is therefore less likely to be felt by small businesses. Small businesses will, however, benefit from no longer having to notify with the supervisory authority and from a reduction in data security breaches through implementing privacy by design.

The Regulation would lead to additional administrative burdens for small businesses. Micro and small businesses are likely to be particularly affected by additional administrative burdens, such as complying with rules on consent, since they will not have the in-house expertise to manage additional burdens and will need to employ external consultants to ensure they are compliant.

SMEs and micro enterprises are exempt from the requirement to carry out data protection impact assessments, employ a data protection officer (DPO), and document all processing activities, unless they carry out regular and systematic processing of data subjects. It is estimated that around 4% of SMEs and micro organisations (approximately 42,000) could be carrying out processing that requires them to appoint a DPO and carry out DPIAs (see annex A). For these organisations the additional compliance measures will be costly.

Annex A shows that there are approximately 187,200 private sector data controllers that are SMEs or micro enterprises. This is the number of UK based small organisations that will be affected by the Regulation, although there will also be additional impacts for small data processors which are not quantified here.

Section A, below, looks at the overall impact of the Regulation on micros and SMEs, while Section B monetises the particular costs and benefits that can be attributed to micros and SMEs. 'Small businesses' refers to all micros and SMEs that are data controllers unless otherwise stated.

##### **A. Overall Impact on growth of micros and SMEs**

The Regulation as a whole is expected to be far more costly for micro enterprises and SMEs than for large enterprises. Micros and SMEs are less likely to benefit from a harmonised data protection regime, but will find it far more difficult to absorb the administrative burdens of the Regulation.

##### ***Reduction in legal fragmentation***

One of the benefits of the Regulation cited by the European Commission is a reduction in legal fragmentation. This reduces the cost of doing business for organisations that have to comply with the data protection laws of multiple member states.

However, a reduction in legal fragmentation is less likely to benefit small organisations because they are far less likely to process data in more than one Member State. Data controllers are only affected by the data protection legislation of another Member State if they are "established" in that Member State.<sup>58</sup> The EU Commission take this to mean that the enterprise has a "branch or commercial agent in that Member State".<sup>59</sup> The Federation of Small Business in their evidence to the Justice Select Committee reported that of their members "very few will export data, so the savings from harmonisation are very small."<sup>59</sup> Table B.1 shows that larger organisations are more likely to have a retail outlet or subsidiary in another Member State compared with smaller organisations. For example, 17% of large retailers have a retail

---

<sup>58</sup> EU Commission Impact Assessment. Annex 9, page 144.

<sup>59</sup> <http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/uc572-i/uc57201.htm>

outlet or subsidiary in at least four other member states, compared with 3% of organisations employing between 10-49 people. Smaller organisations are therefore less likely to benefit from harmonisation.

**Table B.1: Number of EU Member States (other than own) in which the organisation has a subsidiary or retail outlet**

		Number of Member States				
		None	1	2-3	4+	DK/NA
<b>Company Size</b>	<b>10-49</b>	84%	4%	1%	3%	8%
	<b>50-249</b>	74%	7%	5%	6%	7%
	<b>250+</b>	63%	10%	6%	17%	4%

Source: EU Flash Barometer survey 300; Interviewed EU27 retailers with at least 10 employees.

It has not been possible to monetise the benefits of a reduction in legal fragmentation, since it is difficult to estimate how many small data controllers are affected by legal fragmentation.

## **Cost of Compliance**

The prescriptive nature of the Regulation means that micro and small businesses will need to employ external consultants to ensure they are compliant, leading to significant additional costs. In a discussion with small technology companies, the companies all stated that they would need to employ external consultants to ensure general compliance with the Regulation and particularly with the following measures:

- Understanding the definition of personal data and ensuring processing is legal;
- Providing the correct information to the data subject;
- Ensuring that consent is explicit;
- Ensuring compliance with the 'right to be forgotten';
- Ensuring that breaches can be identified and reported;
- Ensuring the correct documentation is maintained.

A particular measure which will be costly for micro and small businesses, but is not quantified below, is consent. The impact assessment showed that the requirement for consent to be 'explicit' is likely to deter investment in technology and advertising companies. The Regulation is therefore likely to be detrimental to growth in the technology sector, if new start-ups cannot secure funding for their business model.

## **B. Monetised Costs and Benefits**

### ***Personal data security breaches***

Small organisations will be affected by the requirement to notify breaches of data security to the Information Commissioner. The Impact Assessment showed that around 11% of small organisations, including micros and medium-sized enterprises, have a personal data security breach each year costing between £15,000 and £30,000.

#### ***Reduction in loss of personal data (benefit)***

The Impact Assessment estimated that the Regulation would reduce data security breaches by 11% as a result of the additional compliance measures. For micros and SMEs, a reduction of 11% is a saving of £34-68 million p.a. in 2012-13 earnings terms.

#### ***Cost***

The cost of reporting a breach was estimated to be between £1,100 and £3,000 for a small organisation (this average included responses from micro, small and medium enterprises). The main Impact Assessment showed that after the reduction in personal data loss (estimated above), small businesses would suffer around 18,000 breaches which would need to be reported. The cost to small businesses of reporting data security breaches is estimated to be between £20 million and £55 million p.a. in 2012-13 earnings terms.

## Notification Fees

Small data controllers will benefit from no longer having to notify with the Information Commissioner. For each data controller, this is a saving of £35 from the notification fee itself and £12.50 from no longer having to complete the notification form. This is a total saving of £9 million in 2012-13; the saving from no longer having to complete the notification form will grow in line in earnings.

## Demonstrating Compliance

The main Impact Assessment estimated that the cost of demonstrating compliance with the Regulation (including maintaining the relevant documentation) would vary for micro and SMEs depending on whether or not processing personal data is an activity 'ancillary' to its main activities. For most micros and SMEs the cost of demonstrating compliance is estimated to be £53 p.a. in 2012-13 earnings terms. However, for the 42,000 controllers classified as carrying out 'risky' processing, the costs will range between £53 and £640 p.a.

Table B.2 shows the total cost of demonstrating compliance with the Regulation. Costs will range between £10 million and £35 million per annum in 2012-13 earnings terms, to reflect the variation in the cost of maintaining documentation. There may also be additional costs to micros and SMEs if they have to employ legal advice to clarify whether or not their processing is classified as an 'ancillary activity'.

**Table B.2: Annual cost to micro and SMEs of demonstrating compliance; 2012-13 earnings terms**

	Unit Cost		
	Low	Best	High
Small controllers not processing data as a main activity	£53	£53	£53
Small controllers processing data as a main activity	£53	£160	£640
	Total Cost (£millions)		
	£8	£8	£8
Small Controllers not processing data as a main activity	£8	£8	£8
Small controllers processing data as a main activity	£2	£7	£27
<b>Total</b>	<b>£10</b>	<b>£14</b>	<b>£35</b>

## Subject Access Requests (SARs)

Small organisations will be affected by the increase in SARs that result from the removal of the £10 fee. The main Impact Assessment estimated that SARs would increase by between 25% and 40% as a result of the removal of the £10 request fee.

However, small organisations are less likely to receive large numbers of SARs compared with larger organisations. An EU Barometer survey found that across all 27 EU Member States 13% of large organisations receive more than 50 SARs a year compared with 6% for organisations employing between 50-249 people and 5% for organisations employing between 20-49 people<sup>60</sup>.

The figures from the EU Barometer Survey above have been applied to the number of businesses in the UK to estimate what proportion of the total cost can be attributed to small business – this is shown in table B.3. The table shows that although only 5% of businesses employing between 20 and 49 people get 50 or more SARs a year, 54% of the additional cost will go to these businesses because they make up 63% of all businesses in the UK employing 20 or more people. Table B.3 shows that the total cost to small and medium enterprises is £10-32 million in 2012-13; this excludes the costs to businesses employing less than 20 people as it has not been possible to monetise these impacts. This cost will grow in line with earnings.

**Table B.3: Additional SAR costs attributed to SMEs; 2012-13 earnings terms**

<sup>60</sup> EU Commission (2008), 'Data protection in the European Union: data controller's perceptions'. Flash Barometer 226.

	<b>Number of Businesses</b>	<b>% getting 50+ SARs</b>	<b>% of Total Cost</b>	<b>Low Cost (£millions)</b>	<b>High Cost (£millions)</b>
<b>20-49</b>	63,670	5%	54%	£6.3	£20.3
<b>50-249</b>	30,475	6%	32%	£3.7	£11.8
<b>250+</b>	6,320	13%	14%	£1.6	£5.1
<b>Total</b>	<b>100,465</b>		<b>100%</b>	<b>£11.6</b>	<b>£37.3</b>

Source: BIS Business Population Estimates 2011 and EU Flash Barometer Survey 226. Only companies employing at least 20 people were included in the survey.

### **Data Protection Impact Assessments (DPIAs)**

The Impact Assessment showed that there are approximately 42,000 micro enterprises and SMEs that could be expected to carry out DPIAs because of the nature of their processing. This is approximately 4% of all SMEs and micro enterprises. The list of affected organisations is given in annex A.

The cost to these organisations of carrying out DPIAs was shown to cost £54-£67 million in 2012-13 earnings terms. The range reflects the uncertainty as to whether micro organisations will have to carry out Data Protection Impact Assessments if their processing is classified as 'regular and systematic'.

### **Data Protection Officers (DPOs)**

As with DPIAs, it is estimated that there are around 42,000 SMEs and micro enterprises that would be affected by the requirement to employ a Data Protection Officer. This was estimated to cost £34-£182 million in 2012-13 earnings terms in the full Impact Assessment, depending upon whether four hours of legal work is sufficient to fulfil the requirements of the Regulation for medium enterprises.

### **Conclusion**

The main benefit of the Regulation to small data controllers is a reduction in data security breaches achieved through a more proactive approach to privacy and data security. Small businesses will also benefit from no longer having to notify with the Information Commissioner. However, small organisations are less likely to benefit from the harmonisation of data protection legislation across the EU since they are less likely to process personal data in multiple member states.

However, the Regulation is likely to be costly for small businesses due to the need to recruit external consultants to ensure compliance. There will also be costs to small businesses through additional SARs and from having to notify data breaches to the Commissioner. It is expected that these costs will outweigh the benefits.

There will be particularly high costs to the 42,000 small organisations that are not exempt from the requirement to employ a DPO, carry out DPIAs and document all processing. For these organisations the costs will be particularly high.

Table B.4 gives a summary of the costs and benefits to small businesses that have been monetised in this test. The cost to small businesses is estimated to be between £80 and £290 million per annum in 2012-13 earnings terms. This cost does exclude the benefit from a reduction in legal fragmentation which it has not been possible to monetise; however, small businesses are expected to be less affected by legal fragmentation compared to large data controllers.

**Table B.4: Annual monetised costs and benefits to small businesses; £millions, 2012-13 earnings terms**

	Small Businesses		
	Low	Best/Mid	High
<b>Benefits</b>			
Reduction in data breaches	£30	£50	£70
No Notification	£10	£10	£10
<b>Total Benefit</b>	<b>£40</b>	<b>£60</b>	<b>£80</b>
<b>Costs</b>			
Notifying breaches	£20	£40	£50
SAR Requests	£10	£20	£30
DPIAs	£50	£60	£70
DPOs	£30	£110	£180
Demonstrating Compliance	£10	£10	£30
<b>Total Cost</b>	<b>£130</b>	<b>£240</b>	<b>£370</b>
<b>Net Benefit</b>	<b>-£80</b>	<b>-£180</b>	<b>-£290</b>

Note: figures have been rounded to the nearest £10million

### Competition Impact

#### Introduction

The EU Commission's Impact Assessment concludes that the Regulation will have a positive impact on economic competitiveness for three reasons<sup>61</sup>:

1. *Reducing the cost of doing business*: harmonisation of EU law will lower the cost of doing business in the EU.
2. *Increasing the capacity to innovate*: harmonisation of the EU law and increased consumer confidence will bring investment into the EU.
3. *Increasing International competitiveness*: harmonisation should encourage internal competition within the EU and strengthened data protection should increase external competition.

The collection and analysis of personal data can enhance the consumer experience by enabling companies to target offers and products at individuals depending upon their preferences. However, the increased collection and use of personal data can also be of detriment to the consumer if data is misused. Whether the Regulation is positive for competition and growth therefore depends on how the law balances the need for businesses to be able to use data to benefit the consumer experience, while ensuring it is adequately protected.

While harmonisation should lead to increased competition and therefore growth within the internal market, there is evidence to suggest that parts of the Regulation could be detrimental to competition and growth in the EU economy. Firstly, the benefits of harmonisation are outweighed by the administrative burdens that the Regulation adds, increasing the cost of doing business in the EU and the UK. Secondly, there is evidence to suggest that a Regulation which is overly burdensome could deter investment in the technology and advertising industry and therefore weaken overall growth.

#### 1. Cost of doing business in the UK

The EU Commission's Impact Assessment concludes that the Regulation will lead to an administrative saving for business of €2.3 billion due to harmonisation across the EU of data protection law. This therefore lowers the cost of doing business in the EU, increases competition and pushes down prices, increasing economic growth.

Full harmonisation of data protection law would lower the cost of doing business where the data controller operates in more than one Member State. Multinational companies support the principle of harmonisation across the EU for this reason, as was reflected in the Call for Evidence - for example:

- Facebook welcomes the principle of a single data protection law across the EU for multinational companies;
- Microsoft argues that a consistent framework across the EU is essential for development of growth and innovation in the EU.
- Adobe provides services in all 27 EU Member States and welcomes replacing the Directive with a Regulation in order to clarify questions of applicable law and jurisdiction and reduce the legal costs of ensuring compliance across all Member States.

However, the Impact Assessment has shown that the Regulation has high administrative costs to business due to prescriptive measures such as the requirement to appoint a DPO and the requirement to notify the supervisory authority of all data breaches within 24 hours. These administrative burdens will increase the cost of doing business, and so will have a negative impact on competition and growth.

These high administrative costs could be particularly detrimental to the competitiveness of the UK economy if they lead to suppliers establishing their business outside of the EU to avoid the high costs of complying with the Regulation. For example, in the UK Call for Evidence Cloud computing companies and Data centres expressed concern about the definition of personal data which would make it far more costly to continue to operate their current business model in the EU.

---

<sup>61</sup> See annex 10 of the Commission Impact Assessment.



The Regulation will also not result in complete harmonisation, since Member States have a wide discretion under the Regulation to derogate from many of the rights and obligations.

## **2. Capacity to innovate**

The internet is an important contributor to growth in the UK economy. In the UK the internet economy is estimated to be worth well over £100 billion, the highest proportion of GDP of any G20 country<sup>62</sup>. The use of data is an important contributor to growth in this sector. For instance, 'Parkopedia' is an example of a new application which uses local data and location data to provide users with information about where they can find free car parking spaces<sup>63</sup>.

The Impact Assessment showed that the Regulation will make it more costly for data controllers to do business and so is likely to limit growth in this sector. There is also evidence to suggest that the Regulation could deter investment and therefore innovation in advertising and the internet industry due to its rules around consent, profiling, definition of personal data and high administrative sanctions. This is likely to be particularly detrimental to the competitiveness of the UK economy, as the UK is a leader in the internet industry.

### *Rules around consent*

Article 4 of the Regulation requires that consent must be "specific, informed and explicit". The requirement for consent to be "explicit" goes further than the current DPA and in the Call for Evidence over half of respondents felt that this would require controllers to give data subjects an "opt-in" for their data to be collected.

In 2012 Booz&co. carried out a survey with 189 angel investors and 24 venture capitalists to understand the impact that changes in privacy regulations could have on their decision to invest in advertising technology companies. While the survey was for the US, angel investors and venture capitalists invested nearly €3.8 billion in Europe in 2010 (around half of which was in the high-tech sector) and so the survey results are relevant to Europe<sup>64</sup>.

The survey by booz&co. found that privacy regulations requiring opt-in before any data is collected would reduce the pool of interested investors in advertising technology companies by 65%<sup>65</sup>. This suggests that the rules around consent could have a negative impact on investment in the internet industry. However, such a survey question is likely to trigger a negative response, and so if consent is not too costly to obtain under the Regulation the impact on investment may not be too detrimental. For example, in a separate survey by Allen and Overy just over half of businesses thought explicit consent would be "manageable", although the number of companies sampled in this survey was very low at just 50.<sup>66</sup>

If the higher standard for consent does limit investment in new internet start-ups then this is likely to be detrimental to growth and competitiveness in the UK, since it will be harder for new businesses to enter the market. Making it costly to enter the market will therefore limit competition for internet services, making these services more expensive for the end-user.

### *Impact on direct marketing*

The direct marketing industry identifies specific characteristics about consumers in order to produce personalised adverts, while advertising agencies use this information to tailor adverts to their receivers.

Article 20 forbids "automated processing of personal data intended to evaluate certain personal aspects". It is not clear whether or not this prohibits behavioural advertising or personalised services, but if it does this is likely to be detrimental to competitiveness in the advertising sector. The Direct Marketing

---

<sup>62</sup> Bartlett, J (2012), 'The Data Dialogue'. A Demos Report.

<sup>63</sup> Deloitte (2012), 'Open Data: driving growth, ingenuity and innovation'. A Deloitte analytics paper.

<sup>64</sup> Ibid

<sup>65</sup> Le Merle et al (2012), 'The impact of US internet privacy regulations on early-stage investment. A quantitative study.' Booz&co.

<sup>66</sup> Allen and Overy (2012), 'Proposed EU data protection regulation: what do people think?'

Association (DMA) estimate that in the UK in 2011 £14.2 billion was spent on direct marketing, utilising profiling techniques; restrictions on this market are therefore likely to be costly to the UK economy<sup>67</sup>.

However, even if behavioural advertising can continue, the higher standard for consent, along with the extended definition of personal data to include online identifiers, is expected to limit the extent to which companies can use direct marketing. DMA (UK) estimate the overall cost of not being able to target consumers directly as a result of the Regulation to be £47 billion<sup>68</sup>. This could weaken UK competitiveness if it leads to lower spending on marketing which, in turn, makes it harder for businesses to sell their goods and services.

Restrictions on consent, profiling and changes to the definition of personal data may also restrict growth in the internet economy due to the limitations they place on web-based advertising. Web services, such as search engines, are able to be provided free of charge because they generate revenue through personalised advertising. If less money were spent on advertising and the adverts were less effective it would reduce the extent to which advertising companies would subsidise such services, which would be detrimental to the end user. This will weaken competition in the internet economy, a field in which the UK is currently a leader.

However, as set out in the Impact Assessment, there may be some advantages to limiting personalised advertising. As companies possess more information they have a greater ability to price discriminate, i.e. offer personalised prices based on their information about the consumer's budget and spending habits. Placing restrictions on behavioural advertising therefore limits the ability of businesses to charge higher prices by targeting those customers with a higher marginal willingness to pay.

#### *Protection of personal data*

Consumers are less likely to engage in certain transactions if they have concerns about the security of their personal data. For example, in 2002 Jupiter Research forecast that \$24.5 billion in on-line sales would be lost by between 2002 and 2006 because of privacy concerns<sup>69</sup>. In The EU Flash Barometer Survey 225 67% of individuals agreed they were worried about leaving their personal information on the net<sup>70</sup>. This suggests that if consumers feel their data is better protected they are more likely to use the internet to make online transactions, encouraging growth in this sector.

However, it is not clear that a Regulation alone will cause EU residents to feel that their data is better protected. In the same Flash Barometer survey, 77% of individuals agreed that awareness of data protection law is low suggesting that the introduction of the Regulation on its own will not necessarily lead to growth for the internet industry because individuals will not be aware of the new requirements on the security of their data.

#### *Administrative sanctions*

As discussed in the body of the Impact Assessment, the Regulation sets out a three tier fine approach for failure to comply with the Regulation. These fines are considered disproportionate to the cost of the harm caused which could have a negative impact on competition and growth.

The objective of a fine is to incentivise data controllers to comply with data protection legislation. However, excessively high fines may lead to data controllers spending unnecessary amounts of money on consultants to ensure they are compliant. In extreme cases, excessively high fines may over-deter by discouraging investors away from markets and practices that could raise the possibility of an infringement action. For example, a survey by booz&co., found that 65% of angel investors and Venture Capitalists agreed with the statement "I am uncomfortable investing in business models in which of amount of damages is uncertain and potentially large"<sup>71</sup>. Excessively high fines will therefore limit

---

<sup>67</sup> DMA (2012), 'Putting a price on direct marketing'.

<sup>68</sup> This figure was calculated from a survey of 600 UK companies who were asked how their businesses would respond if they could no longer use web analytics for marketing purposes. This includes the loss to advertising companies.

<sup>69</sup> Acquisti (2010), 'The economics of personal data and the economics of privacy'

<sup>70</sup> EU Commission (2008), 'Data protection in the European Union: Citizen's perceptions.' EU Flash Barometer survey 225.

<sup>71</sup> Le Merle et al (2012), 'The impact of EU internet copyright regulations on early-stage investment. A quantitative study'. Booz and co.

competition in markets where analysis of personal data is central to the work of the organisation, thus particularly affecting growth in the internet economy

The high fines proposed in the Regulation risk driving a firm out of business. The Federation of Small Business raised this concern in its response to the Call for Evidence, stating that “some of the fines envisaged in the proposal will be significant sums of money to a small business, forcing some of them to close”. If a market already has a small number of competitors then further limiting the number of suppliers in that market could be very detrimental to competition and growth.

### **3. International Competitiveness**

The EU Commission expect that internal competition will increase as a result of harmonisation because businesses will more easily be able to operate across the EU. The EU Flash Barometer survey 300 found that across the EU 31% of companies thought that their cross-border sales would increase if the “laws regulating transactions with consumers were the same throughout the EU”. For the UK, this is true of 27.5% of companies. These survey results imply that harmonisation of data protection laws will enable more companies to compete for business in other member states, lowering prices and increasing economic growth.

The EU Commission also expect the Regulation to increase external competition due to stronger consumer confidence and simplification of transfers to third parties. However, for the UK the Regulation will make internal transfers more difficult. In the UK there is currently no prior-approval mechanism whereby the supervisory authority approves each and every transfer. Under the Regulation organisations will have to put Binding Corporate Rules or a contractual clause in place, approved by the supervisory authority. This is likely to be more burdensome and so increase the cost to business.

The administrative burdens of the Regulation, such as mandatory DPOs, may also deter businesses from investing in the UK compared to non EEA Member States. For example, in the booz&co. survey of angel investors and venture capitalists in the US, 86% of investors said that they would prefer to operate under US privacy law compared with European privacy law<sup>72</sup>. Most companies in the US self-regulate when it comes to data protection. A more prescriptive Regulation could therefore deter investors from investing in UK technology companies compared with those in the US or elsewhere.

### **Conclusion**

The impact that the Regulation will have on competition and growth in the UK is mixed. A move towards harmonisation is expected to be positive for growth and competition as having one law will increase cross-border trade. However, the Impact Assessment showed that the net impact of the proposed Regulation on business is negative. As the Regulation raises the cost to data controllers of doing businesses so this raises the cost of providing goods and services in the UK, weakening UK competitiveness.

There are also parts of the Regulation that make it more burdensome to do business in the UK and so could deter investment in the technology sector. For example, survey evidence suggests that making consent explicit could deter investors. The rules around profiling could also stifle growth in the advertising and internet economies, as could high administrative sanctions.

The EU Commission claims that enhanced protection of personal data will be positive for competition because companies will want to trade in the EU and because consumers will be more willing to engage in internet sales. However, it is not clear that a Regulation alone will be enough to make consumers more willing to share their personal data. Similarly, evidence suggests that companies prefer to operate under privacy laws similar to the US, rather than the more prescriptive EU laws. Therefore, the evidence suggests that the overall impact of the proposed Regulation on growth and competition, as it is currently drafted, is likely to be negative.

---

<sup>72</sup> Le Merle et al (2012), ‘The impact of US internet privacy regulations on early-stage investment. A quantitative study.’ Booz&co.

## **Annex D**

### **Justice Impact Test**

#### **In brief, what is the proposal?**

On 25 January, the European Commission published a proposal for a new Regulation on data protection on which, if adopted, will repeal and replace the 1995 EU Data Protection Directive, which is transposed into UK law by the Data Protection Act 1998 (DPA).

The proposed Regulation will be negotiated by EU Member States and the European Parliament before becoming law. The Justice impact test will accompany an overarching Impact Assessment of the proposed Regulation, alongside other specific impact tests.

#### **What is the proposal intended to achieve, over what geographical area (e.g. England, England and Wales) and in what timescale?**

As set out above, the proposed new data protection framework will be subject to extensive negotiations by EU Member States and the European Parliament before becoming law. Following that process, the earliest the Regulation would come into force is likely to be 2016.

#### **What public commitments have been given and to whom?**

The UK has committed to doing an Impact Assessment and has made stakeholders, Parliament and other EU Member States aware of this.

#### **What are the options under consideration?**

The proposed Regulation, if adopted, would be directly applicable in UK law, and therefore the justice impact test focuses on the impacts of the Regulation in its current draft.

#### **How does the proposal change what happens now? Who will be affected and in what numbers?**

The proposed Regulation would repeal most, if not all of the current DPA.

The new data protection Regulation would affect all organisations ('data controllers' and 'data processors') in all sectors based in the EU, and those outside the EU processing the personal data of EU residents. These organisations will be required to comply with the Regulation's new, more stringent and specific data protection compliance requirements and be liable to greater sanctions, unless a relevant exemption applies. However, the Regulation will not apply to competent authorities processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the processing of personal data for national security purposes, or personal data processing conducted in the course of purely personal or household activities. We estimate that there are around 355,000 data controllers in the UK affected by the proposed Regulation.

The EU residents whose personal data is being processed will enjoy new and enhanced data protection rights as a result of the new Regulation. The population of the EU is around 500 million, of whom just over 60 million live in the UK. It is reasonable to assume that all of these are data subjects.

The UK data protection supervisory authority, the Information Commissioner's Office (ICO), would enforce the new requirements and may need to conduct more investigations and conduct more enforcement action under the more prescriptive rules set out in the proposal.

## 2. Criminal Offences and Civil Penalties and Sanctions

### **Are we creating new civil sanctions, fixed penalties or civil orders with criminal sanctions or creating or amending criminal offences?**

The Information Commissioner currently has the power to impose Civil Monetary Penalties (CMPs) of up to £500,000. The proposals include a three-tier system of administrative sanctions for a wide range of infringements of the Regulation. The highest sanction available to supervisory authorities proposed is either 1m euros or 2% of an enterprise's annual worldwide turnover, which could be as high as several hundred million euros for the largest enterprises. The fear of administrative sanctions may lead to better compliance with the regulation, but on the other hand, as the criteria for issuing sanctions in the proposals is wider than the DPA, it is likely there will be more sanctions than at present. This could lead to increased litigation if those fined choose to dispute the sanctions, which may happen more than at present if a particularly large fine is imposed, given that the ICO's current fining powers are limited to £500,000.

No criminal sanctions are created by the proposals.

### **Details of the relevant legislation**

The Information Commissioner currently has the power to issue CMPs under the DPA and the Privacy and Electronic Communications Regulations 2003 (PECR). The proposed Regulation would bring in new civil infringements and higher fine levels, as set out in the box above.

No criminal penalties are proposed by the EU Commission.

## 3. Courts and Tribunals

### **Do we expect there to be an impact on HM Courts Service or on Tribunals Service (or both) through the creation of or an increase in applications/cases?**

Articles 74 and 75 of the Regulation contain proposals that could mean increased recourse to the courts by individuals and organisations. Article 74 would provide the right to seek a judicial remedy against a decision of a Supervisory Authority. Currently, organisations against whom the ICO has taken enforcement action may appeal to the Information Rights Tribunal. However, individuals do not enjoy a specific right to appeal to the Courts against the decisions of the ICO. It is possible therefore that there will be significant increase in the number of appeals against the ICO. This could be exacerbated by the provision for data subjects to bring proceedings against supervisory authorities in other Member States than where they reside. There is also a right to a judicial remedy against a controller or processor for non-compliance with the Regulation which could further increase the number of proceedings.

Article 75 also envisages a greater possibility for individuals to seek a judicial remedy without the involvement of the ICO where the Regulation's requirements have not been met. Currently, the circumstances where an individual can apply to the courts under the DPA for a remedy are limited to certain situations (for example where a subject access request has not been complied with, where data processing is causing unwarranted damage or distress, or the personal data in question is inaccurate). This opens up the possibility of more data protection court cases than the low number which are heard now, although this is incredibly difficult to quantify.

Article 76 provides that data protection rights organisations may also exercise the above rights on behalf of one or more individuals. Article 77 provides that compensation may be obtained for damage caused by a contravention of the Regulation, although this broadly mirrors the right that individuals currently have under section 13 of the DPA.

Similar rights are provided for in Chapter VIII of the proposed data protection Directive.

These new and amended rights would suggest an increase in the data protection caseload of the courts and tribunals. Furthermore, the proposed Regulation as drafted would bring a number of prescriptive new obligations on data controllers and processors and new and enhanced rights for data subjects that could lead to increased litigation and an increased caseload for the justice system, including the magistrates' courts, county courts and the Information Rights Tribunal. This workload will include the collection and enforcement of fines imposed under the Regulation, and specialist judicial training on the provisions of the new Regulation.

Since the DPA came into force in 2000, 20 enforcement cases have gone to the Tribunal, an average of 1.7 every year. Figures for the Tribunal are not broken down between Freedom of Information and data protection, but even given that, the Information Rights Tribunal hears very few cases overall, compared to many other Tribunals. The total number of cases before them for 2011/12 was 300.

Article 53 of the proposal gives the Information Commissioner the power to access premises of an organisation, although this needs to be exercised "in conformity with Union Law and Member State law". This could mean that the Information Commissioner would still be required to apply for a warrant along similar lines to those available to him under Schedule 9 to the DPA. In the period 2005 to 2012, the Information Commissioner applied to a circuit judge for a warrant for entry and inspection under Schedule 9 to the DPA on average 7 times per year. Given that there may be greater need for investigations under the revised rules and the requirement that the Information Commissioner serve administrative sanctions, these applications may increase in the future.

**Would we expect fewer cases to come to HM Courts Service or Tribunals Service as a result of the proposal?**

We would not expect there to be fewer cases before the Courts or Tribunals as a result of the proposals.

**Does the proposal create a new right of appeal or route to judicial review? If so, how will these be handled (i.e. by the courts/tribunals)?**

Currently, the Information Commissioner's decisions are subject to appeal to the Information Tribunal and, on points of law, to the Courts. Under the DPA, the Information Commissioner can bring enforcement cases to the Tribunal and bring prosecutions against data controllers to the Courts.

As set out above, the proposed Regulation would bring in rights for individuals and organisations to seek a judicial remedy against a decision of a Supervisory Authority. It would also allow an individual to request that the supervisory authority in their Member State take action on his or her behalf against the supervisory authority in another Member State (so for example the French equivalent of the Information Commissioner could be asked to take action against the UK Information Commissioner by a resident of France).

Given the proposals are still being negotiated, no decision has been made about precisely how these rights would be exercised, if they do remain in the final negotiated Regulation.

**Do we expect to establish a new tribunal jurisdiction? If so, has this been discussed with Tribunal Service?**

We do not expect there will be the need to establish a new tribunal jurisdiction. Although no decisions have been made about precise mechanisms for exercising the rights set out above, we would envisage that, under the proposed Regulation, cases would be heard before the same Courts and Tribunals as now.

**Has the use of alternative dispute resolution (ADR) procedures (including mediation) been considered? If not, why not?**

The EU Commission has not indicated that it considered the use of ADR as a formal mechanism.

**Will the proposal require enforcement mechanisms for civil debts, civil sanctions or criminal penalties?**

The future enforcement mechanisms should remain the same as those used now.

**Do we anticipate that Court and/or Tribunal procedural rules will have to be amended? If so, when is the likely date for the changes?**

There may be the possibility of changes to the rules, depending on the content of the final Regulation.

In particular, article 76 requires a court in one Member State to contact a court in another Member State to ascertain whether “parallel proceedings” are taking place. If such proceedings are taking place the court may suspend the proceedings before it.

Subject to the progress of negotiations and agreement on a final text, these changes are likely to be required in 2016.

**Will the proposals require sentencing and/or penalty guidelines to be amended?**

Not directly. Under Article 78 of the proposal, Member States are required to lay down rules on the penalties available for infringements of the Regulation’s requirements. These will therefore be a matter for implementation in domestic law. The Information Commissioner’s guidance on civil monetary penalties would need to be replaced to reflect the new regime.

#### **4. Legal Aid**

**Is our proposal likely to have an impact on the Legal Aid fund?**

Yes, but we think it will have a minimal impact on the civil legal aid budget.

**If legal aid may be affected, will (i) criminal, or (ii) civil and family, or (iii) asylum legal aid be affected?**

It is unlikely there will be an impact on the civil legal aid budget as there is no legal aid available for cases before the Information Rights Tribunal. Legal Aid had been previously available at Legal Help level, in particular for cases involving data protection before Employment Tribunals but this was taken out of scope as a result of legal aid reforms in 2011.

The proposed new Regulation does not create any new criminal offences and so there will be no direct impact on the criminal legal aid budget. If the UK proposed any criminal sanctions as part of implementation under article 78 that could have an impact on the criminal legal aid budget. This would be looked at as part of the implementation process.

**If legal aid may be affected, would legal aid costs increase or be reduced (and by what margin)?**

We do not have estimates for this at present. The Legal Services Commission does not hold separate data on criminal legal aid cases involving data protection. However, the proposed Regulation does not create any new criminal offences and we understand that there are only small numbers of such cases.

## **5. Prisons and Offender Management Services**

**Will the proposals result in an increase in the number of offenders being committed to custody (including on remand) or probation?**

As the proposal does not contain any criminal sanctions, there will not be an increase in the number of offenders committed to custody.

**Will the proposals result in an increase in the length of custodial sentences?** The proposed Regulation does not set down any custodial sentences.

**Will the proposals create a new custodial sentence?**

The proposed Regulation does not create new custodial sentences.

**What do we expect the impact of the proposals on probation services to be?**

There will not be an impact on probation services as a result of the proposed Regulation.



## Annex E

### Equality Impact Test

1. Name of the proposed new or changed legislation, policy, strategy, project or service being assessed.

Proposals for EU Data Protection legislation

2. Individual Officer(s) & unit responsible for completing the Equality Impact Assessment.

Bilal Toure, Domestic Data Protection Team, Information Directorate

3. What is the main aim or purpose of the proposed new or changed legislation, policy, strategy, project or service and what are the intended outcomes?

Aims/objectives	Outcomes
The Commission proposes harmonised data protection law across the EU, applying across the public and private sectors, and which is congruent with current and future technological advances.	Updated and new individual rights in the area of data protection and prescribed rules for public and private sector organisations on their processing of personal data. The proposals also cover the enforcement of the new framework by data protection supervisory authorities (in the UK this is the Information Commissioner's Office)

4. What existing sources of information will you use to help you identify the likely equality impacts on different groups of people?

*(For example statistics, survey results, complaints analysis, consultation documents, customer feedback, existing briefings, submissions or business reports, comparative policies from external sources and other Government Departments).*

The Ministry of Justice (MoJ) ran a Call for Evidence on the proposed EU data protection legislation in February/March 2012. The Call for Evidence invited individuals and those representing specific groups within society to outline their views on the European Commission's data protection proposals (both the Regulation and Directive dealing with the sharing of data on criminal matters, which is not covered in this equality impact test). The Call for Evidence received 143 written responses, including from the Information Commissioner's Office (ICO), Citizens Advice, Microsoft, British Banking Association, a variety of legal firms and members of the public. In addition, MoJ officials took part in various bilateral meetings, round table events and workshops. Several other sources were also taken into consideration, including:

- ICO Annual Track 2011 Report (Individuals);
- ICO Customer Satisfaction Survey (July 2009);
- 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 (2008);
- MoJ Post Implementation Review of the Data Protection Act 1998 Equality Review (January 2011)
- The Flash Barometer 359 "Attitudes on Data Protection and Electronic Identity in the European Union" (June 2011)

5. Are there gaps in information that make it difficult or impossible to form an opinion on how your proposals might affect different groups of people? If so what are the gaps in the information and how and when do you plan to collect additional information?

6.

There are no centrally collated statistics about how data protection legislation affects people along lines of disability, race, gender and gender identity, religious belief, sexual orientation, pregnancy and maternity and caring responsibilities. This makes it difficult to assess how different groups may be positively or adversely affected by any change in the law. However, various surveys on awareness of data protection have grouped respondents by particular characteristics (specifically age, gender and whether they are “white” or “non-white”). The Equality Review conducted by MoJ and published in January 2011 concluded that there was no evidence to suggest that data protection legislation had had an adverse impact on the above groups. Below we present more recent evidence about different groups’ awareness about data protection.

7. Having analysed the initial and additional sources of information including feedback from consultation, is there any evidence that the proposed changes will have a **positive impact** on any of these different groups of people and/or promote equality of opportunity?

Please provide details of which benefits from the positive impacts and the evidence and analysis used to identify them.

The data protection proposals provide a framework that is not specific to disability, race, sexual orientation, gender or any other of the protected characteristics.

Like the 1995 Data Protection Directive (95/46/EC) the proposals place a general prohibition (subject to exemptions) on the processing of personal data of certain special categories. These categories are:

- Race or ethnic origin;
- Political opinions;
- Religion or beliefs;
- Trade-union membership;
- Genetic data;
- Data concerning health;
- Sex life;
- Criminal convictions;
- Related security measures.

The new proposals have added to the existing list of special categories by adding genetic data. The 1995 Directive also refers to “religious or *philosophical* beliefs” so it may be that data on a greater range of beliefs is offered protection by this amendment.

At the same time, Article 9(2) of the proposed Regulation allows organisations to process sensitive personal data for the purposes of carrying out the obligations and exercising the specific rights of the controller in the field of employment, in so far as it is authorised by Union or Member state law. This could include processing of sensitive personal data for the purposes of promoting equal opportunity and diversity in employment. This provision is broadly similar to one contained in the 1995 Directive and should continue to help raise the awareness of imbalances in the employment of different groups.

Article 11 of the Regulation provides a provision for transparency in information and communication. This provision places a responsibility on the data controller to provide information to the data subject on how their information is processed and the policies the data controller has in place in regard to the processing of personal data. This article is explicit in its requirement for data controllers to provide a response to data subjects who wish to know how their data is being used in an ‘intelligible form, using clear and plain language, adapted to the data subject’. In particular, it should be adapted for children, if they make requests. This provision should help to ensure that there is no restriction based on disability or age when it comes to the data subject requesting information on how their personal data is processed.

The ICO is the independent regulator of the Data Protection Act 1998 (DPA), which gives effect to the existing 1995 Directive. As part of its functions, the ICO produces yearly reports and studies which hold key information on data protection demographics (on the basis of the existing domestic and EU

legislative framework) that have been used to inform this assessment. This equality impact test is about the European Commission's proposals as published in January 2012, which if adopted, would not come into force until 2016 at the earliest. For the purposes of considering the equality impact however, we have out of necessity used the statistics from the current data protection framework to benchmark the possible effects the proposals may have on equality. We have analysed the ICO's 2011 Annual Track report produced by Social Market Strategic Research (SMSR), which contains information about individuals' awareness of the DPA and broader information rights and their attitude to disclosing personal data about themselves.

The annual track 2011 survey was conducted between 8<sup>th</sup> August to the 3<sup>rd</sup> September 2011, where 1241 individuals were surveyed over the phone. Quotas were placed on individuals by age, gender, region, ethnicity and socio-economic grouping to ensure a nationally representative sample was achieved.

#### Awareness

According to the ICO 2011 Tracker survey awareness of the right to see information among respondents aged 18 to 24 was 12% lower than average (54% compared to the 66% average), awareness among respondents in this age group has increased by 12% since 2010.

Consistent with the 2010 Track report, those aged 25 to 34 indicated the highest levels of spontaneous awareness (56%) of the DPA. Only 17% of those aged 65 and over reported awareness and awareness among this age group has decreased by 7% since 2010.

To ensure awareness of the proposals the decrease amongst older individuals will have to be taken into consideration before the enactment of the proposed legislation, there is a high possibility that people within this age group may not be aware of the changes in data protection law. It is difficult to draw definite conclusions about what this lack of awareness means. The 2011 MoJ Equality Review of the DPA suggested that it might be due to the withdrawal from work life and the fact that this generation grew up in an age when data processing was less widespread. If the latter was the case, one would expect an increase in awareness in this age group over time.

#### Attitudes

The Special EU Barometer Flash 359 provides some interesting statistics on Europeans aged 15-24, and students, although these statistics are for all Europeans and not just UK citizens. The survey found that young Europeans in this group are most likely to agree that disclosing personal information is not a big issue for them (43%, EU 33%) and that they do not mind disclosing personal information in return for free services online such as a free email address (48%, EU 29%).

The same survey also found that young Europeans aged 15-24, usually do not read privacy statements on the Internet (31%, EU 25%), but they do feel sufficiently informed about the conditions for data collection and the further uses of their data when joining a social networking site or registering for a service online (64%, EU 54%).

The ICO 2011 Tracker survey also highlighted that males are more likely to request personal information held by an organisation. 18% of males said they had requested information compared to 10% of female respondents. This indicates that almost twice as many men than women make subject access requests and so are more likely to benefit from the removal of the fee. The 25 to 44 age group is the most likely to assert their rights and request personal information (17%), which has remained the case since 2009. It may be the case that the proposed Regulation would increase the level of requests for personal information from organisations made by females through the abolishment of the £10 fee for subject access requests, but we have no evidence to suggest that the fee is currently dissuading women more than men.

8. Is there any feedback or evidence that additional work could be done to promote equality of opportunity? If the answer is yes, please provide details of whether or not you plan to undertake this work. If not, please say why.

There is no evidence, based on statistical studies, desk research, stakeholder workshops and responses to the recent Call for Evidence to suggest that further work needs to be done in this sphere to promote equality of opportunity.

However, as the negotiations progress, and as the date from which the new data protection framework will apply comes closer, the UK Government will keep the equality issues that are raised in this screening under review.

9. Is there any evidence that proposed changes will have an **adverse equality impact** on any of these different groups of people? Please provide details of who the proposals affect, what the adverse impacts are and the evidence and analysis used to identify them.

Overall, the proposals would affect all data subjects whose data is being processed in the context of the activities of an establishment of a controller or a processor in the Union. It would also apply where a data controller not established in the Union processes the personal data of data subjects residing in the Union where the processing consists of the offering of goods or services to such data subjects or monitoring their behaviour.

Aside from this, there is no evidence that the changes will have an adverse equality impact on any of the different groups.

10. Is there any evidence that the proposed changes have **no equality impacts**? Please provide details of the evidence and analysis used to reach the conclusion that the proposed changes have no impact on any of these different groups of people.

Based on the survey evidence above and responses to the MoJ's Call for Evidence there is no positive evidence to suggest that the proposals will have no impact on equality.

11. Is a full Equality Impact Assessment Required? Yes ☐ No ☒

If you answered 'No', please explain below why not?

The impacts identified above, such as they are, suggest a minimal impact on equality. The proposals are intended to apply to all, regardless of age, gender, sexual orientation or the other characteristics highlighted above.

In addition, the EU negotiations over the new proposals are ongoing and so the draft is subject to change. It would therefore be disproportionate at present to conduct a full Equality Impact Assessment. However, as the implementation of the new data protection framework comes closer, the UK Government will keep the equality issues that are raised in this screening under review.

12. Even if a full EIA is not required, you are legally required to monitor and review the proposed changes after implementation to check they work as planned and to screen for unexpected equality impacts. Please provide details of how you will monitor evaluate or review your proposals and when the review will take place.

It is expected that the new data protection framework will not apply until 2016. The new rules will be subject to post legislation review in the normal ways. In addition, the periodic surveys mentioned above will continue to consider awareness and use of data protection rights among different groups within the population.

13. Name of Senior Manager and date approved

Name (must be grade 5 or above): Glenn Preston

Department: Information and Devolution Policy, Ministry of Justice

Date

Note: The EIA should be sent **by email to [analyticalservices@justice.gsi.gov.uk](mailto:analyticalservices@justice.gsi.gov.uk) of the Equality Analytical Programme for publication.**