



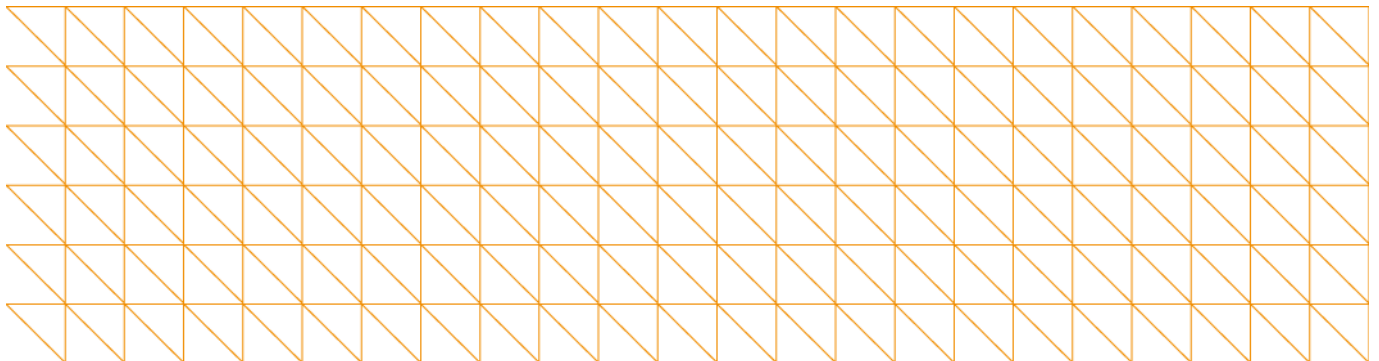
Ministry of
JUSTICE

Summary of Responses

Call for Evidence on Proposed EU Data Protection Legislative Framework

Summary of Responses to Call for Evidence on the Proposed EU Data
Protection Legislative Framework

This Summary of Responses is published on 28 June 2012





Ministry of
JUSTICE

Summary of Responses

Call for Evidence on Proposed EU Data Protection Legislative Framework

Summary of Responses to Call for Evidence on Proposed EU Data Protection Legislative Framework carried out by the Ministry of Justice.

This information is also available on the Ministry of Justice website:
www.justice.gov.uk

About this consultation

To: All interested parties, members of the public, organisations

Duration: From 07/02/12 to 06/03/12

Enquiries (including requests for the paper in an alternative format) to: Bilal Toure
Ministry of Justice
102 Petty France
London SW1H 9AJ

Tel: 020 3334 3555

Email: informationrights@justice.gsi.gov.uk

Contents

Introduction and contact details	2
Background	3
Summary of responses	6
Responses to specific questions	9
Conclusion and next steps	34
The consultation criteria	36
Annex A – List of respondents	38
Annex B - Checklists	
Regulation - checklist for analysis on EU proposals	45
Directive - checklist for analysis on EU proposals	66

Introduction and contact details

This document is the Summary of Responses to the Call for Evidence on the Proposed EU Data Protection Legislative Framework.

It will cover:

- the background to the Call for Evidence;
- a summary of the responses to the Call for Evidence; and
- details of the next steps.

Further copies of this report and the consultation paper can be obtained by contacting **Bilal Toure** at the address below:

Justice Policy Group
Ministry of Justice
102 Petty France
London SW1H 9AJ

Telephone: 020 3334 3555

Email: bilal.toure@hmcts.gsi.gov.uk

This report is also available on the Ministry's website: www.justice.gov.uk.

Alternative format versions of this publication can be requested from informationrights@justice.gsi.gov.uk

Background

The European Commission ('the Commission') published new legislative proposals for data protection on 25 January 2012. The proposals contain a Regulation (for general and commercial data protection) and a Directive (covering processing in the areas of police and criminal justice). The draft Regulation is intended to repeal and replace the 1995 Data Protection Directive (95/46/EC), which is implemented into UK law by the Data Protection Act 1998 (DPA). The draft Directive will repeal and replace the existing Data Protection Framework Decision (2008/977/JHA) (DPFD), which was agreed in 2008 and applies to Police and Judicial Co-operation in Criminal Matters.

The proposals for a new Regulation in the area of data protection came about as the 1995 Data Protection Directive is widely perceived to be out of date. Since 1995, there have been numerous technological developments, notably the increased use of computers, the expansion of the internet and the emergence of social media networks which have seen changes to the ways that personal data are handled and processed.

The Ministry of Justice launched a Call for Evidence on the proposals on 7 February 2012, which closed on 6 March 2012. The Call for Evidence sought information on the potential impact of both the draft Regulation and draft Directive. This document is a summary of the written responses the Ministry of Justice received. The evidence received, in addition to that gathered in discussions, seminars and roundtables with a range of interested parties, will help to assist the UK's position in the ongoing negotiations at EU level.

Summary of key areas from the Regulation

The draft Regulation builds on the 1995 Data Protection Directive, with the aim of strengthening online privacy rights and boosting the economy. There are benefits to individuals in the shape of new and increased rights but also new obligations for organisations who process personal data. Overall, it will be important to consider the impact, including costs and benefits, of the proposals on both individuals and data controllers.

The Commission's proposals include an updated definition of personal data, which now explicitly mentions online identifiers, locational data and genetic data. The rules around consent have also been changed, requiring consent to be explicit.

The proposals also contain a requirement for organisations to report data breaches without undue delay and, where feasible, within 24 hours to the regulator, a requirement to conduct data protection impact assessments, as well as a requirement for some organisations to appoint a data protection officer.

The Commission proposes abolishing the fee which organisations may charge for subject access requests (currently a maximum of £10 for most cases). It has also introduced a proposal for a new 'right to be forgotten', under which, in certain circumstances, individuals can request the erasure of their personal data which an organisation holds. Where the data has been made public a controller is required to take all reasonable steps to inform third parties that the data subject has requested erasure of their data.

It is proposed that national supervisory authorities will have the power to take action against organisations in other EU Member States in certain situations. Supervisory authorities will also be able to sanction specified breaches of the Regulation and will be able to issue fines of up to €1m or up to 2% of a company's annual turnover in some cases.

The proposals build on the existing mechanisms (as set out in the DPA's eight principles) and provide a detailed framework for international transfers of personal data. There are also requirements for supervisory authorities to undertake prior checks of some types of transfers. The derogations which data controllers can use have also been changed, and are more restrictive than those currently in place.

Summary of key areas from the Directive

The Commission proposes to include domestic processing within the scope of the Directive (for example data transferred between two regional police forces with no cross-border element). The 2008 Data Protection Framework Decision (DPFD), which the Directive replaces, only covered cross-border data transfers and not processing of personal data carried out within the borders of a single Member State.

As with the proposed Regulation, the definition of personal data has been updated by referring to online identifiers, locational data and genetic identity.

The proposals include new rights of access and information for data subjects, such as the identity of the data protection officer, and the period for which the data will be stored. There is also a new right for data subjects to directly demand the erasure of their personal data by the data controller. The DPFD also imposed obligations in respect of erasure, but gave Member States discretion as to whether the right could be asserted directly against a data controller. The Commission proposes a new obligation for data controllers to implement 'appropriate technical and organisational measures and procedures' in order to ensure the protection of the rights of the data subject.

It is important to be clear that the Government does not consider that the provisions relating to domestic processing will apply to the UK.

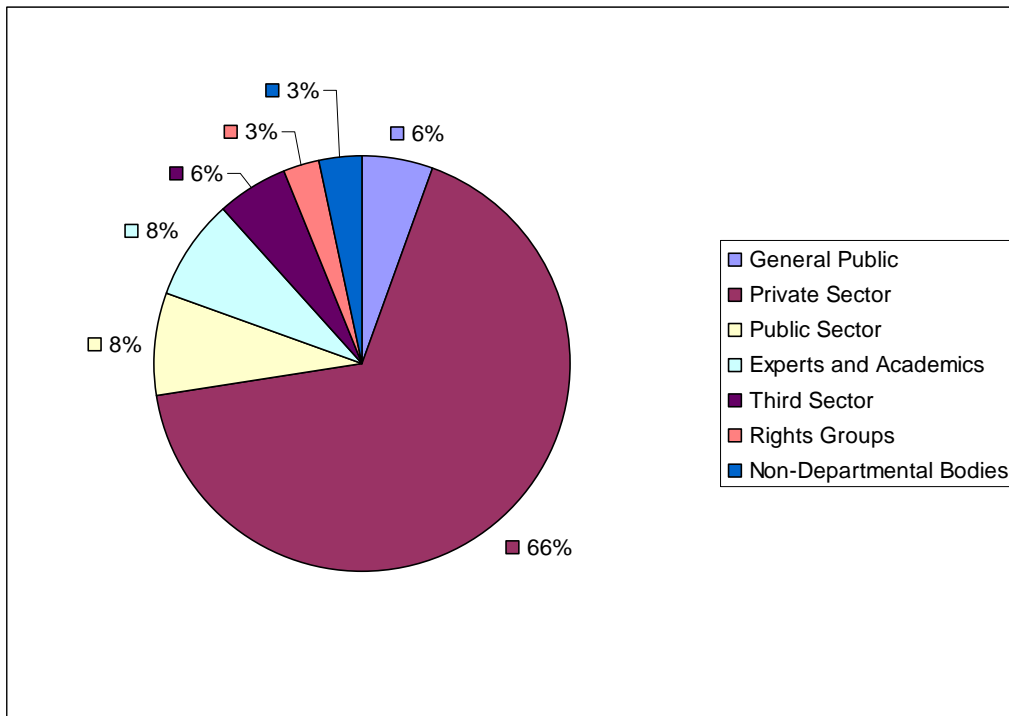
There is a proposal, similar to that in the Regulation, which requires data controllers to inform supervisory authorities and data subjects of personal data breaches. It requires informing the former without undue delay and where feasible not later than 24 hours after discovery; the latter are to be notified when the personal data breach is likely to adversely affect the protection of

personal data or privacy and should be done 'without undue delay'. The notification of the breach shall not be required where the controller can establish that technical measures were in place making the data unintelligible to anyone with unauthorised access to the data. The proposed Directive requires data controllers and data processors to designate a data protection officer.

A list of respondents to the Call for Evidence is at Annex A.

Summary of responses

The Call for Evidence received a total of 143 written responses. The respondents included a range of organisations from all sectors, consumer and rights groups as well as the general public. A sector-specific breakdown of responses can be found in the chart below:



Call for Evidence on the Proposed EU Data Protection Legislative Framework:

Summary of responses

Sector	Responses
Advertising	5
Business (other)	7
Education	1
Expert (information rights) and academics	11
Financial (insurance and credit reference)	19
Government department	2
Health care sector	6
IT, telecoms and ICT	20
Legal	17
Local government	2
Media, communications and social media	10
Members of the public	8
NDPB	5
Other (includes children's interest groups and charities)	8
Police	2
Research (includes medical research)	7
Retail	3
Citizens and consumer rights groups ('Rights groups')	4
Small and Medium Enterprises and representatives	2
Telecoms	2
Utility	2
Total	143

To complement the written Call for Evidence, MoJ officials also met representatives from a range of industries and rights groups, both in bilateral discussions and in roundtables. These have been important in gathering views on the proposals, and we have been particularly grateful for those events organised externally to which we have been invited. These sessions have proved thought-provoking and have helped to inform the Government's position on the proposals.

The written responses to the Call for Evidence were logged and filed upon receipt by the Ministry of Justice. The Data Protection policy team then considered the responses and summarised them in one summary document. This and the original responses were analysed by policy officials. This analysis is reflected in this document.

Respondents to the Call for Evidence naturally expressed varying views on specific parts of the proposed Regulation as well as the current Data Protection Act 1998 (DPA). Not all respondents provided information about the impact the proposals would have on them, but chose instead to describe issues surrounding the legislative framework currently in place. We welcome these views and have noted them, but they are not reflected in this summary

document as our present aim is to gauge the impact the Commission's proposals would have on the UK. Where possible, this summary document has tried to reflect the majority view but where a particularly important point was put across by a small proportion of respondents (for example, members of the general public) we have included these as well.

Importantly, it should be noted that the overwhelming majority of the responses received to the Call for Evidence addressed the proposed Regulation, rather than the Directive. This summary document therefore focuses on the proposed Regulation.

Impact Assessment

The checklists included at Annex B represent the Ministry of Justice's best assessment to date of the likely impact of the proposals. The checklists refers to the proposals as published on 25 January 2012 and do not reflect any changes to either draft instruments that will be agreed through negotiations.

The Commission published an Impact Assessment to accompany the draft Regulation and the draft Directive. This estimated that the proposals would together bring about a net benefit of €2.3 billion per annum. This net benefit arises from savings achieved through data controllers no longer having to comply with the rules of different member states and through an end to notification fees.

It is the view of the Ministry of Justice that the Impact Assessment produced by the Commission does not properly quantify the costs which would be imposed on business through compliance with the proposals while potentially over-estimating the benefits achieved through having a harmonised legislation across the EU. The Impact Assessment does not assess the cost of many measures that will have an impact on business (including small businesses), such as strengthened subject access rights and the 'right to be forgotten', while also under-estimating the cost of those measures that are quantified, such as the cost of compulsory Data Protection Officers in large corporations and those processing 'risky' data.

In the coming months the Ministry of Justice will be working to try to better quantify the costs and benefits of the Commission's proposals on the UK economy. This work will focus on the measures likely to have the greatest impact on businesses and citizens in the UK, while also seeking to better understand the benefits that come about by having a single data protection law for the EU member states. This assessment of the impact will help to inform the UK's negotiations with the EU and in line with the Government's commitment to transparency, it is our intention to publish our analysis. It is the Government's current intention that this will be by the end of this calendar year, but this does depend on the pace and scope of the negotiations on these proposals.

Responses to specific questions

The Call for Evidence attracted a wide range of general responses about the proposed Regulation. The majority of respondents recognised the need for change in the data protection legislative framework, and that the proposed Regulation would be a start at improving the existing legislation. Members of the public and rights groups, in particular felt that the Regulation addressed key consumer concerns and gave individuals more rights to control how their personal data was processed.

However, a large number of public and private sector organisations thought that the proposed Regulation would represent an administrative burden that lacks a proper balance between the rights of individuals and the legitimate needs of data controllers, and is overly prescriptive in some areas. They also commented that there was ambiguity in the drafting. Particularly widespread concerns were expressed about the introduction of a ‘right to be forgotten’, data breach notifications being reported within 24 hours where feasible, and the imposition of large fines for data controllers who failed to comply with the Regulation’s requirements.

Some respondents believed that the proposed Regulation did not take into account technological changes over the last few years, such as the growth of the internet, the widespread uptake of social networking sites and the increase in the use of geo-location data. Many thought that it would place overly-ambitious requirements on all data controllers by using a ‘one size fits all’ approach without understanding the various needs that businesses have for specific types of personal data and the flexibility needed to provide a range of services to their customers. Social media companies, credit reference agencies and e-commerce businesses in particular have argued that the proposed Regulation will have a negative impact on the core functions of their business.

Respondents, mainly from the private sector, felt that the proposal is too complex to understand without the aid of additional, and possibly expensive, legal guidance.

“Our initial assessment of the implications is that the additional requirements beyond EU 95/46 currently proposed will result in significantly increased complexity and cost that will outweigh any potential cost-savings in the areas indicated by the Commission.”

Telecoms sector response

Finally, one of the reoccurring themes in responses to the Call for Evidence has been the emergence of cloud computing and the potential threat that the proposed Regulation brings to innovation in this area of technology. Various respondents argued that, as it stands, cloud computing represents a new and economically viable way of processing data in any part of the world. This means it has become easier for countries outside the UK's jurisdiction to process data belonging to EU citizens. Respondents have suggested that by introducing a prescriptive Regulation, the EU runs the risk of hindering a generation of technological innovators.

Chapter I: General Provisions

This chapter sets out the scope and the definitions used in the proposed Regulation.

Article 3: Territorial scope

Article 3 of the proposed Regulation would widen the reach of EU data protection law, covering not only organisations processing personal data within the EU, but also those outside the EU who process the personal data of EU residents when offering goods or services to them, or monitoring their behaviour (for example via website cookies).

Not many respondents addressed the issue of territorial scope as set out in Article 3. However, there were consistent concerns from the majority of those who did address it, with respondents questioning how it would be implemented in practice. They also suggested that this would raise false expectations for data subjects resident in the EU about the level of protection actually afforded to their personal data when being processed by data controllers in non-EU countries.

“Clarification is required in respect of how this increase in territorial scope is to be regulated and how it is to apply to the concept of cloud-based processing.”

IT sector response

The key question for many respondents was one of enforcement. They noted that the proposal has not set out an enforcement mechanism for non-EU data controllers who infringe the Regulation's requirements. This means that a realistic deterrent has not been put in place to ensure that non-EU organisations comply with the Regulation.

“For some businesses, however, the requirement may be extremely problematic. Organisations may be subject to other laws in their own jurisdiction in addition to EU data protection law. In some cases these laws may conflict with EU law, and organisations may have difficulty determining which law takes precedence. Moreover, there is no obvious enforcement mechanism which could be employed in respect of businesses operating from outside the EU.”

Legal sector response

That said, the majority of respondents agreed that, in principle, the application of Article 3 would be a good thing, if it were achievable. Respondents felt that such scope would give data subjects assurance that their personal data has the same level of protection globally as it has in the EU. They commented that such a proposal would help other, non-EU countries adopt robust data protection principles. This would encourage consumers to engage with more online services, strengthen e-commerce and increase the level of trust between data subjects and online service providers.

The emergence of cloud computing was raised in this context by several respondents. They felt that the European Commission, through trying to regulate personal data that is processed completely outside the EU, would be imposing new regulation, that previously did not exist on the cloud and its customers. Respondents felt that this could result in the opposite to what many governments have said they are trying to achieve, by over-regulating an emerging technology that could stimulate global economic growth.

Article 4: Definitions

The vast majority of respondents to the Call for Evidence expressed concerns over some of the definitions used in the proposed Regulation. Respondents felt that some key definitions were in danger of being left open to interpretation and were not specific enough to address issues in relation to industries such as the information technology sector which process vast amount of information comprising of IP addresses and cookies. The definitions covered below are those which attracted the most significant comment.

Personal data and data subject

The vast majority of respondents felt strongly that there is a need for clarity on the definition of personal data. Many respondents remarked that the proposed Regulation has brought online identifiers, locational and genetic data into scope of data protection legislation. On the one hand, businesses felt that the definition put forward by the Commission does not take into account the context or circumstances in which personal data may be used. By making the definition of personal data so broad, they argued that they would be so inhibited by rules so as not to be able to provide services to their customers. On the other hand, it was argued by others, in particular rights groups, that by making the definition of personal data as broad as possible, data subjects will be assured that they have control over (and protection for) the information they provide to organisations.

Most respondents commented on the ambiguity of the definition of personal data, when coupled with Recital 24 which states that: *'identification numbers, location data, online identifiers or other specific factors...need not necessarily be considered as personal data in all circumstances'*. Most Respondents from the legal sector have asked for clarity as Recital 24 seems to contradict Article 4 and could lead to legal uncertainty as to when and for whom information is, or is not, personal data.

Respondents from the information technology industry argued that an internet protocol (IP) address does not necessarily identify a person, but rather a device that uses the IP protocol. These respondents pointed out that the nature of IP addresses means that an address can either be dynamic or static, and in most cases addresses tend to be dynamic. This means that each time an individual makes an online connection, the IP address would be different from the one they used the last time they went online.

These respondents argued that by explicitly bringing IP addresses into the scope of data protection legislation, security could be compromised as the Regulation would apply to network information, such as an IP address, which is used to monitor and stop criminal activity and the data subject could request this information to their advantage. An individual who has committed or intends to commit a criminal act online could request from a company if his or her IP address is known to that company, before they carry out an illegal act.

"For example a cyber criminal once informed of such processing will be aware that its attack has been detected and could simply change the malware being used to avoid further detection. The simple act of informing the cyber attacker could inhibit security providers from stopping an attack and could jeopardise possible law enforcement investigations and endanger law enforcement's ability to capture attackers due to the fact that the criminal has been made aware that the attack has been identified"

IT sector response

Filing system

A minority of respondents commented on the definition of a filing system and the term 'structured set of personal data'. These respondents suggested that this means that 'unstructured personal data' is therefore outside the scope of the Regulation (in contrast to the UK's Data Protection Act 1998 (DPA) as amended by the Freedom of Information Act 2000). Rights groups have argued that if this is the case, the Regulation could reduce the rights of individuals, such as access and correction when personal data is processed in an unstructured format or filing system by a public authority. This would be the case in particular in the areas of social work, housing, education, and health. These respondents suggested the Regulation should be changed to maintain the protection of unstructured personal data which is already subject to the UK's data protection regime.

Main establishment

A few respondents commented on the definition of what determines the main establishment of a data controller (*'the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken'*). They commented that this definition does not take into account the dynamic nature of business models and the ongoing changes to business structures where decision-taking is not necessarily centralised. Respondents have asked if the term 'main establishment' could be more clearly defined, explicitly setting out how a main establishment would be determined. This was viewed as particularly important if the Commission's goal of achieving a one-stop shop for data controllers is to be achieved, given that the main establishment would determine which supervisory authority oversees the processing of that data controller.

The data subject's consent

There were mixed views from respondents on the Regulation's definition of the data subject's consent as *'any freely given, specific, informed and explicit indication of his or her wishes'*. Some respondents felt that the introduction of the term 'explicit' has provided clarity in understanding the meaning of consent, in the context of data protection compliance.

Over half of the respondents felt that the use of the term 'explicit' in this context would require data controllers to provide data subjects with an 'opt in' to the processing of their personal data, where this processing was based on the consent of the data subject. This would be a particular difficulty when data controllers needed to comply with the requirement to gain consent for placing 'cookies' on users' equipment under the Privacy and Electronic Communications Regulation 2003 (as amended).

It was noted by many respondents on this point that consumers would like an internet service that is fast, easy-to-use and efficient. They believed that the introduction of consent as 'explicit', read alongside the conditions set out in Article 7 (see below), could undermine consumer concerns and needs by requiring numerous opt-in mechanisms on websites. This could potentially frustrate many internet users and ultimately lead them to opt in as a matter of routine (so-called 'consent fatigue'), even in cases where their privacy would be better served by opting out.

Chapter II: Principles

This chapter sets out the principles which data controllers must follow when processing personal data along with the conditions for legitimate processing, the conditions for consent and the conditions for processing sensitive personal data.

The Regulation proposes new elements in the processing of data, which includes a transparency principle and further details on data minimisation and retention including reviews for data stored for longer periods for research purposes.

Article 5: Principles relating to personal data processing

Relatively few comments were received on the principles set out in Article 5. However, the requirement that personal data be ‘limited to the minimum necessary’ (in Article 5(c)) was welcomed by rights groups, who felt that it would give assurances to individuals that only the minimum amount of their personal data would be used by data controllers to provide a service. However, data controllers who responded indicated that this proposal would have a financial impact on them, particularly in ensuring the ‘legacy’ data they currently hold complies with this requirement as well as current data. One particular organisation quoted on estimated cost:

“Compliance with the data minimisation principle would cost in the region of £10-15 million”

Media sector response

Other organisations who responded were concerned about the implications of both the minimisation requirement and the need to keep personal data up to date for their respective sectors. Notably, respondents from the credit reference industry and archives sector thought that these strict requirements would have an adverse impact and needed some form of softening.

Article 7: Conditions for consent

In relation to Article 7(1), some respondents from a range of sectors stated that it would be difficult for data controllers to prove that a data subject has consented to the processing of their personal data. Some of the respondents touched on the lack of explanation of the phrase ‘burden of proof’ and therefore have assumed that the burden of proof is a physical copy of a data subject’s acceptance to a consent statement. If this is the case, respondents have stated that they would have to factor in additional printing and storage costs for their consent statements, which would be a considerable burden, especially for small and medium enterprises (SMEs), which may not have the resource to accommodate the provision.

Respondents from rights groups as well as members of the public have urged that data controllers should not publish ‘opt in’ statements that are lengthy and full of legal terminology. It has been suggested by companies that data controllers should seek alternative context-specific means and measures to obtain consent rather than simple ‘opt in’ or ‘opt out’ mechanisms.

“With the burden of proof now with the data controller it may be that every challenge by a consumer (or organisation acting on the consumer’s behalf) will require, in the case of a credit reference agency search being challenged, a copy produced of the original consent obtained by our client at the time they carried out the search of our database. This may prove very costly, highly bureaucratic and time consuming for both us and our clients should organisations such as claim management companies target such activity”.

Financial sector response (credit reference agency)

Article 8: Processing of personal data of a child

Less than a quarter of our overall responses commented on Article 8. Respondents agreed with the principle of the Regulation’s intention to provide protection for children’s personal data. However, respondents felt that the definition of a child’s age (as set out in Article 4) was somewhat confusing, as a child is referred to as being under 18 in Article 4(18) but the rules on children’s processing set out in Article 8 only apply to under-13s. Respondents questioned how the European Commission was able to justify 13 as being the minimum age for consent to the processing of data when offering information society services and wanted an explanation of the disparity between this provision and the definition in Article 4.

Rights groups who responded argued that Article 13 of the UN Convention on the Rights of the Child could be used by children to subvert the proposal’s consent requirements:

Article 13: ‘The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice’.

Rights groups specifically commented that the proposed Regulation has not provided derogations for specific online services targeted at children’s welfare and support where a child, for obvious protection reasons, would not want to ask their parent or guardian for consent. Indeed, some respondents suggested that it may be appropriate to require parental consent only where the website provider intends to use children’s personal data for direct marketing or behavioural advertising rather than bring all websites offering children information society services into the scope of this provision.

Several respondents were concerned about the achievability of obtaining verifiable consent, especially in an online context. One respondent commented that the implementation of Article 8 could itself contravene the data minimisation requirements in Article 5. By asking for verifiable parental consent, data controllers would hold parental personal data as well as the child’s personal data, which could be seen as excessive processing.

“simple exchanges will require a disproportionate effort on the part of the child and the parent. For example if the child wishes to sign up for an email newsletter from a children’s programme, this would necessitate the collection, not just of the child’s email address, but also the name and contact details of the child’s parents”

Media sector response

Chapter III: Rights of the Data Subject

The proposals within this chapter set out the rights of a data subject. Under the new proposals, data subjects have more data protection rights than is the case under the existing Directive. These rights range from free of charge subject access requests, the right to be forgotten and erasure and data portability.

Article 12: Procedures and mechanisms for exercising the rights of the data subject

Currently in the UK, data controllers may charge a fee of up to £10 when a subject access request is made (although this may be higher or lower in some cases depending on the type of record). The proposed Regulation would make subject access requests (and similar data protection rights) free of charge with the exception of those which are ‘manifestly excessive, in particular because of their repetitive character’.

Overwhelmingly, rights groups and members of the public who responded to the Call for Evidence agreed with the proposed change to make subject access requests free of charge. They argued that this step strengthens people’s right to be able to request the information that is held about them or potentially affects them.

“We support the requirement for controllers to provide information to the data subject for free and within a reduced time frame. However, we believe that greater guidance is required on what constitutes a vexatious request”.

Rights group response

However, businesses and other organisations have not welcomed the removal of the ability to charge a fee. These groups have predicted an increase in the volume of subject access requests they receive if the fee is abolished, which would have detrimental effects on resource capabilities and budgets. Public sector organisations in particular have commented that they currently feel under strain with the amount of subject access requests they receive. They suggest that the proposal to abolish the fee will leave them stretched and possibly prioritising subject access requests over other similarly important pieces of work, so as to avoid the substantial administrative penalties set out in Article 79.

Many of the responses which covered Article 12 asked the European Commission to clarify the term ‘manifestly excessive’ and ‘repetitive character’ in this context. Respondents felt that this terminology, used to exempt data controllers from responding to subject access requests free of charge, is ambiguous and may need to be set out in more detail. Rights groups felt that if the Commission does not provide this clarity, data controllers may use the terms as carve outs to exempt them from responding to a subject access request. On the other hand, businesses and organisations felt that by having ill-defined terms, data controllers may find themselves either undertaking responses which fall outside the scope of the requirements or failing to undertake responses which fall within scope, and subsequently being fined.

“It could be estimated that there would be a minimum rise in such requests of around 40%. This will significantly impact resource, and will have obvious cost implications.”

Business sector response

Article 17: Right to be forgotten and to erasure

Article 17 of the proposed Regulation gives individuals the right to request that organisations delete their personal data in certain circumstances. Where an individual makes such a request and the personal data has been made public, data controllers are responsible for taking all reasonable steps to inform any third parties that process that personal data that the data subject wishes them to erase that data and any subsequent links to the data.

The consensus from the majority of respondents to the Call for Evidence was that this provision places unrealistic expectations on data controllers, not only to erase all the personal data that they hold on data subjects, but also, where that data has been made public and replicated online, to try to secure its deletion by third parties. Respondents felt that the proposed Regulation has not taken into account the online ecosystem, where data is replicated in seconds. In some instances that personal data becomes ‘viral’, making it almost impossible, they argue, for data controllers to contact third parties in order to erase the personal data in question or links to that data.

Over half the respondents to the Call for Evidence expressed concern at a lack of clarity in the proposed Regulation on how data controllers should implement Article 17. These respondents repeatedly questioned how data processors are expected to validate a request to be forgotten and what mechanisms should be used to substantiate that the request is genuinely coming from the data subject and not from a fictitious source.

Respondents also felt that ambiguity in the terms of the provision could result in data subjects not fully understanding the effects of a 'right to be forgotten', and therefore having personal data erased permanently without the ability to reinstate the data. Alternatively, some respondents thought that the right to be forgotten could be used to conceal an illegal act, and prevent fraud investigators from carrying out their jobs.

“Our clients underline how potentially dangerous the right to be forgotten can be with regard to other fundamental rights, such as freedom of expression, or the legitimate right to build a data-centric business. These rights must in all cases be balanced. We strongly suggest that the provisions of the Regulation should reiterate the rights that are already contained in the OECD Guidelines and the 1995 Directive, which give data subjects the right to rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Regulation”

Legal sector response

A variety of respondents from different sectors stressed that this right may present challenges for data controllers where there are competing legal obligations. For example, financial data may be processed for one purpose but also caught under a requirement to be processed for another, such as the requirements of anti-money laundering regulation.

Respondents from the business sector touched on the financial impact that the 'right to be forgotten' could have on businesses, in particular the cost of changing their business processes to implement the new requirements. Some businesses have estimated costs of up to £100,000. They believe that these requirements will have detrimental effects, as well as place an unnecessary burden on SMEs, who may not have the resources to comply with many of these requests.

However, consumer rights groups welcomed Article 17 as a step in the right direction for consumers who should have the right to have their data removed. They also believed the obligation on data controllers to alert third parties that they should delete the personal data is a progressive move in giving consumers more power to manage their personal data.

“We think that the inclusion of the provision requiring the controller to go to reasonable lengths to alert third parties, such as app developers, that they should delete the information is vital and sets this right apart from the right of the data subject to object to processing”

Rights group response

Article 18 of the proposed Regulation provides data subjects with a right to data portability and the right to obtain their data in a structured, commonly used electronic format. There was an even split in responses to this provision. The business sector was opposed to the idea, whereas rights groups and those members of the general public who responded welcomed it.

Respondents in the latter group felt that the right to data portability was a move forward in data protection rights. Members of the general public felt that Article 18 would give them the power to own their personal data. Likewise, consumer groups believed that the Article would give consumers leverage over service providers to compete, which could result in better pricing and better services for consumers.

Rights groups pointed towards the UK Government's Midata initiative as a platform for the implementation of Article 18. Under Midata, consumers are given access to their personal data from some organisations in a portable, electronic format.

"This emerging ability for individuals to manage their own data for their own purposes has the potential to unleash significant personal, social, civic and economic benefits. With the right support it can encourage the rise of a wide range of new information services, working on behalf of the individual, to gather, analyse, store, process, use and share their data to make better decisions and manage their lives better. These new services are a potential source of economic growth in their own right, and will also enable much more efficient data sharing with existing data controllers."

Data protection expert response

However, the general view from the business sector was that Article 18 moves the Regulation away from the fundamentals of data protection and takes it into the area of consumer protection. Respondents from business felt that this provision would be very draining on resources and costly, particularly for SMEs, who may be inundated with requests from data subjects to have their personal data made available to them in an agreed format for reuse. Businesses were particularly concerned that Article 18 has not left provision for data controllers to protect their trade secrets and intellectual property rights. Businesses also believed that if a single electronic format for data portability was required, businesses would need to modify their existing technology and other aspects of their services, which could result in less functionality, less diversity and a worse user experience.

In terms of a quantified impact, businesses that responded expressed the view that if they were to implement Article 18 the financial burden would far outweigh the benefits of its intent. They gave estimated costs of between £100,000 to £5,000,000 for compliance with this provision. Businesses felt that these costs would inevitably be passed onto customers, who would see a rise in prices for services.

“Whilst we estimate that we would make £4000 per year in direct savings from no longer having to notify our processing activities to the Information Commissioner’s Office (ICO), data protection by design, data portability and the right to be forgotten, would cost an estimated £5 million.”

Media sector response

Article 20: Measures based on profiling

Respondents welcomed the principle behind Article 20, but have asked for clarity on terms such as ‘a measure which produces legal effects’ and ‘significantly affects [a] natural person’. Respondents’ comments reflected those of the Information Commissioner’s Office (ICO), which mentioned in its analysis of the proposal that:

“It is not obvious whether profiling carried out to deliver content to an individual, for example, through behavioural advertising, falls within the scope of this Article”.

Information Commissioner’s Office response

The majority of respondents from the advertising sector felt that the Regulation has failed to clarify whether behavioural advertising or personalised services fall within scope of Article 20. However, on the assumption that behavioural advertising is within scope, respondents felt that the proposed Regulation has not taken into account the significant benefits of advertising in terms of the revenue it brings into the economy and the improvements it has made to people’s online experience. Respondents noted that if the Regulation was to bring behavioural and personalised service advertising into scope of Article 20 and make it impossible to function, there is the potential for there to be a detrimental impact on an industry worth £15.9bn in expenditure.

On the other hand, members of the public and rights groups felt that it is a fundamental right for data subjects not to be subject to measures based on profiling. Those members of the public that responded felt that the Regulation could help to diminish the volume of unsolicited emails being sent to them. They also felt that the measures against profiling in Article 20 are an appropriate mechanism to safeguard vulnerable people from adverts that aim to exploit naivety and difficult personal situations for financial gain.

Chapter IV: Controller and Processor

This Chapter concerns the general obligations of controllers and processors. The regulation sets out specific obligations for controllers arising from the new principles such as data protection by design and by default, which intends to ensure that the processing of personal data is conducted in a way that meet the requirements of the Regulation, and ensures the protection of the rights of the data subject.

Article 23: Data protection by design and by default

The proposed Regulation includes requirements based on the concepts of data protection by design and by default. 'Data protection by design' (also known as 'Privacy by design') is a concept that involves taking data protection into account in the design of systems and procedures. 'Data protection by default' requires that mechanisms are established by the data controller so that the minimum amount of processing of personal data takes place.

Over half of the responses from the Call for Evidence generally welcomed data protection by design as a principle but requested clarity on the practical requirements of the principle. There were three broad splits in opinion on how effective the requirements of Article 23 would be, from rights groups, business and social media businesses.

"We fully support the principle of data protection by design and default. The Article ensures that the principles of data protection are built into systems while not requiring those systems to be overhauled immediately. Over time this should help ensure that data protection is inherent to all systems and processes"

Rights sector response

Civil rights groups felt that Article 23 would give the general public assurance that data protection will be inherent in the design of systems used to store and process data. This meant therefore that consumers could have confidence that their personal data is being protected to a high standard and processed at the minimum level required for its purpose.

"DP officers will have to monitor the implementation of the principles of data protection by design and data protection by default."

The ERA notes that these terms are not defined in the regulation and are therefore open to interpretation. If we are to be judged against these terms, the regulation needs to say exactly what it thinks they mean, otherwise what is required in order to achieve compliance will not be clear."

Telecoms sector response

Respondents from business felt that data protection by design is a good idea in principle. Social media businesses stated that privacy already plays a part in the design of their systems. They pointed out that the foundations of their industry are based on the sharing of personal information. However their view was that an overly strict implementation of Article 23 could mean social media sites would find themselves being non-compliant with the Regulation, which would lead them to being penalised and could ultimately limit the functions of their business.

In terms of financial impact, businesses have stated that the costs of implementing Article 23 far outweigh the proposed savings. They have argued that existing systems would have to be redesigned to take account of the new requirements, which would mean additional costs. Businesses have also questioned whether legacy systems will be within scope of the Regulation. If so, they believe the Regulation should take into account the effect it would have on finances and resource for SMEs as well as large corporations in having to make adaptations to their systems and processes. One business estimated that it would cost £15 million to cleanse its data to the bare minimum of what is needed, in line with a strict interpretation of data protection by design.

Article 25: Representatives of controllers not established in the Union

The majority of respondents to the Call for Evidence, mostly from the public and private sector, felt that the Article 25 is over-ambitious and would not achieve its aim of protecting the personal data of EU residents. As the ICO has pointed out in its analysis of the proposals:

“A controller established in a third country with an adequate level of protection could breach the requirements of the Regulation without necessarily breaching the law of the third country in which it is located”.

Information Commissioner’s Office response

The views expressed by the ICO have been echoed by over half of those who responded, who would like this Article to be rethought.

Articles 31 and 32: Notification of a personal data breach to the supervisory authority and to the data subject

A high proportion of responses covered the issue of data breach notifications, with the prevailing view being that notification of personal data breaches is necessary. However, businesses and other organisations felt that the requirement that states that ‘the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority’ is disproportionate and an unrealistic target to aim for.

The main arguments against such notifications, as set out in the proposal, are that data subjects and the ICO will become inundated with data breach notifications which could result in ‘notification fatigue’. Some respondents argued that if too many routine notifications are sent to data subjects and the ICO, there could be a possibility that high level breaches would go undetected in the midst of a plethora of low level breach notifications. Respondents have proposed that the regulation should seek to remedy some of these difficulties by introducing a trigger or threshold that clearly sets out the requirements needed to notify individuals of a data breach. As the proposed Regulation

stands, there is no mechanism in place to determine or filter out high level or low level data breaches from the requirement to notify.

Many also expressed the view that 24 hours is an over-ambitious window for data controllers to investigate a possible data breach, which could involve data forensic officers and other third party organisations providing intelligence into the nature of the breach. These respondents felt that 24 hours is simply not enough time to determine if a data breach has occurred, and if so who was involved and the scale of the breach. Overwhelmingly, respondents have asked that the Regulation adopts the use of 'without undue delay' rather than 'not later than 24 hours' as an approach to responding to data breaches.

"24 hours is not always sufficient time to gather all the facts and assess all the implications of a personal data breach as required in paragraphs (c) to (e). Would there be a method of voiding the breaches if they were found not to be? Would the ICO be adequately resourced to deal with the volumes of breaches being reported"

IT sector response

In this context, respondents from the IT and Telecoms sector pointed out that they are currently fulfilling similar requirements under the revised e-Privacy Directive (2002/58/EC, as amended by Directive 2006/24/EC and 2009/136/EC), which states that data breaches should be reported to Data Protection Authorities 'without undue delay'. Respondents have requested that the Regulation and the e-Privacy Directive should be consistent in their approach.

"To ensure consistency across data controllers, requirements on breach notification should be unified; if requirements are to be introduced in the Regulations, the relevant provisions of the E-Privacy Directive 2002/55/EC should be repealed"

Telecoms sector response

Respondents have welcomed the Regulation's stipulation that notification to the data subject is not required where the compromised data has been encrypted. Respondents have argued that encrypted data posed no risk to the data subject as the data could not be accessed by third parties.

Respondents felt that there would sometimes be a need to inform affected data subjects of a breach first, so they could take appropriate remedial action, before notifying the supervisory authority and questioned whether this was permitted by the current draft of the provisions.

A very substantial majority of respondents from the private and public sectors commented on the administrative burden the application of Article 32 would have. Respondents believed that they would have to spend more money on training staff and making provisions for changes in organisational processes.

However, members of the public and rights groups welcomed the proposed Article in its entirety. Both groups expressed the view that there are far too many data breaches that go unnoticed and unreported, either to consumers or to the ICO.

"We fully support the proposals as set out in this Article and call on the Ministry of Justice to support them in its discussions in Europe. We are particularly supportive of the provisions to ensure that adequate and consistent information is provided in notifications."

Rights group response

Article 33: Data protection impact assessment

Over a quarter of respondents welcomed the use of data protection impact assessments as a useful mechanism to provide an appropriate level of data protection as well as ensuring accountability and responsibility for data controllers.

"These reforms, and others like them, will help keep data safe. But we believe that certain changes will help to make these responsibility obligations even more robust."

IT sector response

However, a small group of respondents were concerned about the proposal's requirement to inform the supervisory authority of the results of certain data protection impact assessments and to consult data subjects when one is being conducted. These respondents believed that the proposed Regulation has not taken a holistic approach to company structures. One particular company said that it undertook 2000 privacy impact assessments in a single year; they questioned how the supervisory authorities will cope with approving this sort of volume of data protection impact assessments in future.

The same has been said for data subjects who would be consulted when a data protection impact assessment is going to take place. The suggestion from some respondents was that this may lead to data subjects being inundated with consultation requests, which they would not take seriously and may possibly see as a nuisance. Businesses and other organisations also expressed their concerns with data protection impacts assessment being public documents, which may expose business strategies and give competitors an advantage over them.

Finally, a small number of respondents have asked the Commission to clarify the statement that a data protection impact assessment should be undertaken when processing takes place in a 'large-scale filing system'. Respondents felt that without a clearer definition of 'large-scale' some data controllers will not know whether there is an obligation to produce a data protection impact assessment or not.

Article 35: Designation of the data protection officer

There was a substantial volume of responses to Article 35. Respondents from rights groups and members of the public welcomed the need to have independent data protection officers in organisations where personal data is being processed. However, both rights groups and businesses have questioned the effectiveness of the designated data protection officer. Respondents felt that there is a risk that data protection officers could be sidelined in organisations as they are meant to be autonomous of the organisation. Questions also arose about what powers the data protection officer would have in a jurisdiction outside the EU and what sanctions and fines a data protection officer could enforce.

Overwhelmingly businesses have expressed their dissatisfaction with Article 35 and the associated costs that would come with it. The majority of these respondents felt that Article 35 is a clear example of where the Regulation is overly prescriptive. Again, respondents were concerned that the requirement does not take into account the complexities of a company's hierarchical structure, which could potentially see the data protection officer having to ask for further resources to carry out their functions.

In looking at the scope of the provision, many believed that it should focus on the sensitivity of the data being processed rather than the amount of employees. As drafted, the requirement applies to public sector bodies and to enterprises employing 250 persons or more, irrespective of the sensitivity of the data they process. Respondents have asked what happens where a company falls short of employing 250 members of staff, but frequently processes large quantities of personal data.

Equally, where smaller organisations are within scope (as their core activities 'require regular and systematic monitoring of data subjects') respondents felt that designating an independent data protection officer was a disproportionate obligation on businesses. Respondents felt that the requirement may have damaging effects on SMEs, as data subjects may feel that companies that have not designated a data protection officer may not have an adequate level of data protection. Therefore they may move their custom to larger organisations which are able to designate and employ a data protection officer, but which may nonetheless not provide a good level of data protection. Some respondents also commented that the proposed Regulation seems to engage employment law by prescribing the length of time an organisation has to employ a data protection officer and the terms and conditions of their employment, which respondents thought was an overly-prescriptive approach.

As an alternative, some respondents have argued in favour of the ICO's suggestion of a chief policy advisor who is a senior executive with the ability to influence decisions.

"However, we do not believe that data protection officers, of the form envisaged in the proposed Regulation, need necessarily be mandatory, provided that organisations have effective processes in place for ensuring data protection compliance"

Information Commissioner's Office response

Chapter V: Transfer of Personal Data to Third Countries or International Organisations

Chapter V sets out the conditions which data controllers and data processors must meet if they wish to transfer personal data outside of the European Economic Area (EEA). Most of the chapter builds upon the existing mechanisms currently in operation in addition to providing a legal base for international transfers.

Article 40: General principle for transfers

A large proportion of respondents agreed with the principle behind the Regulation's rules on international transfers outside the EEA. Respondents welcomed the need to have a harmonised approach when it comes to making data transfers outside the EEA which is effective and sustainable, while maintaining a strong data protection ethos.

However, respondents felt that the articles in this chapter will result in an overly bureaucratic process, which could stifle growth in industries which heavily rely on outsourcing the processing of data outside the EEA.

Equally, a large number of respondents felt that due consideration has not been given to the ramifications of the proposed Regulation on the current Model Clauses or the Safe Harbor arrangements with the United States, which would need to be updated in light of the changes brought in by the proposed Regulation (although it should be noted that transitional provisions for such arrangements are included in Articles 41(8) and 42(5)).

Article 42: Transfers by way of appropriate safeguards

A large number of respondents felt that prior authorisation by the supervisory authority for outsourcing contracts based on non-standard provisions (required by Article 42(4)) would be very onerous, would greatly increase the administrative burden and could lead to delays in outsourcing transactions, whilst data controllers waited for approval of the contract.

“The requirement to obtain prior authorisation is disproportionately burdensome and bureaucratic and could adversely affect our contractual negotiations with suppliers based in third countries if the ICO is unable to consider our clauses in a timely fashion.”

Media sector response

In addition, it was strongly felt by the majority of respondents that the ICO will be inundated with requests for authorisation of contracts, whereas now it does not require data controllers to submit contracts for its approval. It was suggested by some that national data protection authorities, like the ICO, do not have the resources to engage in detailed analysis of the adequacy of complex outsourcing and data transfer contracts. Respondents generally felt that data controllers themselves would be best placed to provide the adequacy assessments needed to provide the proper legal grounds for transferring personal data by way of appropriate safeguards, as required by Article 42.

Article 43: Transfers by way of binding corporate rules

Just under half of respondents were concerned about the impact that the proposed Regulation might have on data processing contracts and agreements that have already been authorised under Directive 95/48/EC. Respondents were concerned that the Commission has not taken into consideration the time and resource organisations have already put into agreeing existing contracts, and that these would not be recognised further to the Regulation coming into force.

“We do not believe that supervisory authorities need to have a role in authorising or approving binding corporate rules – they should, though, be required to offer guidance and assistance to those drawing up BCRs”

Business sector response

Article 44: Derogations

The majority of respondents welcomed the new derogation for transfers which are necessary for the purposes of the legitimate interests pursued by the controller or processor where the transfers are not classed as ‘frequent or massive’ (Article 44(1)(h)); however respondents asked for a clearer definition of ‘frequent or massive.’ Respondents, especially those who represented Cloud computing services, asked that the proposal take into consideration the sensitivity of the personal data being transferred, rather than purely the quantity and frequency of the transfer.

“While a ‘legitimate interests’ justification for transfers might be helpful, using the test of ‘frequent or massive’ as the arbiter for a derogation does not necessarily add any useful clarity to the issue; the focus should be on appropriate safeguards rather than the size or frequency of transfers.”

Legal sector response

Chapter VI: Independent Supervisory Authorities

Chapter VI obliges Member States to establish an independent supervisory authority. This is in line with the current situation, and the supervisory authority for the UK is the Information Commissioner's Office (ICO). Supervisory authorities would have similar duties and powers to now, such as promoting awareness to the public of data protection issues, hearing and investigating complaints and ordering an organisation to rectify, erase or delete data in respect of a breach of the law. However, there are some additional duties and powers.

Most respondents did not provide evidence on this chapter, whilst those that did, with the exception of the ICO, only commented in very general terms. The main points raised about this area focused on the Regulation's reliance on national supervisory authorities (such as the UK's Information Commissioner) to ensure compliance with its requirements and the overwhelming responsibilities the Regulation would place on them. Respondents questioned the ICO's ability to fulfil the Regulation's requirements given the breadth of the processing activities that the Regulation applies to. The general perception by respondents was that the ICO would be unable to keep up with the demand to respond to requirements such as receiving breach notifications, approving international transfers of personal data and reviewing the results of data protection impact assessments.

"DPAs may quickly find themselves overwhelmed by notifications, impairing their ability to effectively tackle the truly serious breaches"

Business sector response

The ICO on the other hand welcomed the requirements for complete independence and adequate resource. However, it has echoed the same views expressed by other respondents in confirming that the Regulation will have considerable resource implications on his office and that Member States would have to be committed to funding adequately the ICO's obligations, as set out in the Regulation. The Information Commissioner has also commented that if the duties placed on his office do not correlate with the resources provided to him, the Regulation will promise protections and duties which his office cannot deliver. The ICO argues that without adequate resources, the knock-on effects of not being able to deliver on its obligations to businesses and to individuals may cost the ICO its credibility as a regulator.

"We are though concerned about the totality of the duties placed on supervisory authorities by the Regulation. This will have considerable resource implications which need to be thought through by member states"

Information Commissioners Office response

Chapter VII: Co-operation and Consistency

Chapter VII sets out in detail how supervisory authorities will co-operate with each other where needed, such as where an organisation is processing personal data in several Member States. It introduces more explicit rules on mandatory mutual assistance, for instance, obliging supervisory authorities to conduct joint investigations and enforcement measures where required.

The chapter also introduces a consistency mechanism for ensuring uniformity of application in relation to processing operations which concern data subjects in several Member States.

Article 57: Consistency mechanism

As with Chapter VI, very few respondents commented in detail on the proposals for EU-wide co-operation and consistency mechanisms. However, rights groups which responded supported the establishment of an independent European Data Protection Board (EDPB). It was felt that the EDPB would be able to provide support to the public in regards to differences of opinion between supervisory authorities when it comes to grey areas in data protection rules. These groups argued that the EDPB will provide one of the fundamental goals of the Regulation, which is harmonisation across Member States. They argued that the EDPB will be able to provide a consistent message to Member States as well as provide support to national supervisory authorities in carrying out their duties.

“The Group considers the establishment of an EDPB to be a welcome development which would allow data protection authorities to communicate frequently, take decisions together and ultimately seek to ensure harmonisation across the EU”

Legal sector response

Businesses who responded commented generally, rather than in specific terms on the co-operation and the consistency mechanisms set out in the proposal. However, although business respondents stressed that they would like to see greater consistency from Member States when global data protection issues need to be addressed, some commented that the establishment of the EDPB seems to leave a question mark on the role and powers of national supervisory authorities and which would have greater authority when it comes to determining domestic issues. They argued that the establishment of an EDPB does not seem to have taken into account the political and social context of each Member State.

Chapter VIII: Remedies, Liability and Sanctions

This chapter sets out the rights of individuals to lodge a complaint with any supervisory authority in any Member State if they believe that a controller has not complied with the Regulation. It also details a new proposal that any body, organisation or association which aims to protect data subjects' rights can act on behalf of data subjects, either with the supervisory authority or via the courts, and allows supervisory authorities to instigate proceedings on behalf of a data subject.

Article 73: Right to lodge a complaint with a supervisory authority

Many respondents welcomed the specific right for data subjects to raise complaints with supervisory authorities, and in particular rights groups welcomed the possibility of organisations or associations raising complaints on behalf of individuals. However some respondents commented on a data subject's ability to look to a number of supervisory authorities to gain a preferred response to a complaint, which could undermine the harmonisation which the Regulation is intended to achieve.

"[We are] concerned that data subjects could "forum shop" on the basis that they think they may get a more favourable outcome if they complain to a particular supervisory authority"

Business sector response

Article 77: Right to compensation and liability

A minority of respondents commented on Article 77, with rights groups in favour of the broadening of compensation to include awards for those data subjects who have suffered 'damage' as a result of unlawful processing or an action incompatible with the Regulation.

This was reiterated by a respondent who asked for the proposed Directive, relating to processing in the areas of police and criminal justice, to ensure an adequate mechanism is in place under that instrument to allow individuals to seek redress and compensation for damages suffered as a result of a data breach made by a competent authority. No such mechanism is apparently proposed in the Directive.

Article 79: Administrative sanctions

A large proportion of responses commented on Article 79, with rights groups and the general public in favour of the introduction of the power for supervisory authorities to impose fines of up to 2% of an 'enterprises' annual worldwide turnover. These groups saw the fining powers as an effective precautionary measure that will remind those who process personal data of their obligations under the Regulation.

“We welcome the addition of administrative sanctions to the tools that the DPA have at their disposal to effectively regulate. In particular we welcome the use of the term “the supervisory authority shall impose” which provides for a mandatory minimum sanction as opposed to the discretion to employ sanctions.”

Rights group response

However, business and organisations have criticised the fining powers as being excessive. The maximum fine a supervisory authority can impose is, in some cases, €1m or, in the case of an enterprise up to 2% of its annual worldwide turnover. Businesses have argued that the maximum levels of these fines are disproportionate, especially when they are available for contraventions such as not completing a data privacy impact assessment or not notifying a data breach within 24 hours. Businesses and organisations agreed that there needs to be some form of penalty when there has been a breach of the Regulation’s requirements, but it should be proportionate to the contravention and the harm caused to data subjects.

“Members feel that the maximum fine of 2% of the annual worldwide turnover is disproportionately high in relation to the risk of harm to an individual that might arise from a breach of the GDPR. One member could potentially face a fine of up to £1,367 million and another unnamed global bank estimates their fines could reach \$1.6 billion.”

Finance sector response

Chapter IX: Provisions Relating to Specific Data Processing Situations

This chapter sets out further rules and some exemptions from the Regulation. The proposals set out the conditions for processing personal data for historical, statistical, and scientific research purposes as well as conditions for publication of research containing personal data.

Articles 81 and 83: Processing of personal data concerning health and processing for historical, statistical and scientific research purposes

Respondents who commented on Articles 81 and 83 were predominantly from medical and research institutions. These respondents welcomed the recognition that processing in these contexts needed special consideration, but asked for further guidance on the scope of processing intended to be covered, especially on medical and pharmaceutical grounds. Respondents suggested that the proposed Regulation should take note of previous events such as the influenza pandemic, where sharing of personal data for research purposes was fast tracked.

Researchers from the medical and health care sector asked for clarity in the area of processing pseudonymised (key-coded) data, which plays a substantial role in medical research. Respondents have questioned if pseudonymised data is in scope of the proposed Regulation.

Researchers commented that they often found themselves at odds with the UK's DPA, which they argued did not allow them to gain access to patient details. They suggested that in situations where the public interest in research is a priority, it can become necessary for researchers to share personal data and to have clear guidance setting out the derogations from general data protection rules that will achieve this.

Chapter X: Delegated Acts and Implementing Acts

Chapter X sets out the powers of the Commission to adopt delegated acts to supplement the Regulation. It also contains the provision for appropriate Committee procedures.

The majority of respondents commented on the Commission's proposed ability to make delegated and implementing acts (in approximately 45 circumstances).

A small number of respondents referred to the Commission's powers to make delegated acts as "Henry VIII clauses". Respondents felt that such provisions will inevitably lead to legal uncertainty. Respondents, mostly from the legal sector, commented that the use of delegated acts will have a huge impact on their ability to advise their clients. An example given was that businesses that would like to undertake long-term planning through consultation with legal advisors could not be given assurances whether the decisions they make today, even on the basis of the Regulation, will be compliant in five or 10 years time.

Both business and rights groups have requested further clarity on the Commission's process for adopting delegated or implementing acts and whether there would be consultations with data protection authorities or businesses before such implementing acts are made. Rights groups stressed the importance of ensuring that stakeholder engagement is at the forefront in the writing and debating of delegated acts.

A small number of respondents commented on the Commission's intention to make three implementing acts per year. With the number of occasions on which the Commission is empowered to make delegated and implementing acts, it has been argued that it could require up to 15 years for industry to gain real certainty on how to apply the Regulation in tandem with delegated acts. Respondents recommended that the number of powers should be reduced.

Responses from the business sector that commented on the proposed delegated acts highlighted the possible costs for industry as a result of the Commission dictating the technological format and specifications that should be used. Businesses used the example of implementing acts in relation to data portability, where an industry may have developed policies and procedures to address portability concerns. The Commission's power to specify the "electronic format" and the technical procedures and standards that should be used for data portability, would effectively undermine the measures developed by an industry and the investment they have already made in this area, leaving them at a financial loss.

Conclusion and next steps

The Ministry of Justice is grateful for the wide range of responses that have been submitted in response to this Call for Evidence. We would like to thank the individuals, groups and organisations who have taken the time to contribute.

Many respondents to the Call for Evidence have asked that the legislation should take into account the evolving nature of technology and its growing dependence on personal data. Fundamental technological advances such as social networking and cloud processing have brought a new dimension to the ways in which personal data is processed, especially by making it easier for data subjects to transfer their data internationally for it to be stored and processed in different parts of the world. Responses to the Call for Evidence have highlighted the need for a Regulation that is consistent with future technological advances, but at the same time it must safeguard effectively people's right to data protection.

The Government will negotiate at EU level for an instrument that does not overburden business, the public sector or other organisations, and that encourages economic growth and innovation. However, this must be achieved at the same time as ensuring that people's personal data is protected. With these guiding principles in mind, and backed up by the information provided in response to the Call for Evidence, the UK Government will:

- support the provisions requiring transparency of processing, including the new transparency principle and the requirements for data controllers to provide accessible and easy-to-understand information about processing;
- support the requirement for additional information to be provided to data subjects both proactively and in response to subject access requests (subject to consideration of the additional costs), but resist the proposal that subject access rights be exercisable free of charge;
- push for an overhaul of the proposed 'right to be forgotten' given the practicalities and costs and the potential for confusion about its scope for both organisations and individuals; however, the Government reaffirms its commitment to the right for individuals to delete their personal data, where this is appropriate;
- resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals; examples of this include mandatory data protection impact assessments, seeking prior authorisation from the supervisory authority for certain processing operations and the mandatory designation of independent data protection officers;

- support the introduction of data breach notifications both to supervisory authorities and affected individuals, but only if the provisions reflect the timescales needed to properly investigate a breach and if a sensible and proportionate threshold is provided which excludes minor and trivial breaches from the scope of the requirement;
- reaffirm its commitment to a strong and independent supervisory authority at national level and support the establishment of a consistency mechanism to ensure a degree of harmonisation in the application of data protection rules across the EU, whilst allowing independent national authorities some flexibility in how they use their powers;
- support a system of administrative penalties for serious breaches of the Regulation's requirements, but push for a more proportionate level of maximum fines, which allows supervisory authorities greater discretion in applying the powers available to them;
- push for the removal of many of the powers for the European Commission to make delegated and implementing acts, particularly where these have the potential to make a big difference to fundamental requirements and principles (for example, the legitimate interests upon which data controllers can rely to make their processing lawful or the safeguards that must be established to allow profiling to take place).

The negotiations in the Council of the EU and in the European Parliament are ongoing and are likely to last until 2014. During this time, as new proposals and amendments are put forward, the UK Government may seek additional evidence from stakeholders and interested parties. Assuming that texts can be agreed by the European Parliament, the Council and the Commission, Member States, including the UK, will need to consider how best to implement the legislation (although the Regulation will be directly applicable, some provisions are likely to need to be addressed by domestic legislation).

Consultation Co-ordinator contact details

If you have any comments about the way this consultation was conducted you should contact Sheila Morson on 020 3334 4498, or email her at: sheila.morson@justice.gsi.gov.uk.

Alternatively, you may wish to write to the address below:

**Ministry of Justice
Consultation Co-ordinator
Better Regulation Unit
Analytical Services
7th Floor, 7:02
102 Petty France
London SW1H 9AJ**

The consultation criteria

The seven consultation criteria are as follows:

1. **When to consult** – Formal consultations should take place at a stage where there is scope to influence the policy outcome.
2. **Duration of consultation exercises** – Consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.
3. **Clarity of scope and impact** – Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.
4. **Accessibility of consultation exercises** – Consultation exercises should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.
5. **The burden of consultation** – Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.
6. **Responsiveness of consultation exercises** – Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.
7. **Capacity to consult** – Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

These criteria must be reproduced within all consultation documents.

Annex A – List of respondents

Seven responses from member of the public

Absolute Software Corporation

ACPO Scotland

Adobe

Advertising Association

Amberhawk

American Express

Aon Corporation

Archives and Records Association

Ascent Consultants

Association for UK Interactive Entertainment

Association for Financial Markets in Europe/British Bankers Association (joint response)

Association of the British Pharmaceutical Industry (ABPI)

AstraZeneca PLC

AXA Insurance UK plc

BBC

BP

British Retail Consortium

British American Business and British American Business Council

BSkyB

BT

bwin.party digital entertainment plc.

Call Credit

Care Quality Commission

Carnegie Mellon University (research paper)

CBI

Centre for Socio legal studies, Balliol College

Centrica (British Gas)

Children's Charities' Coalition on Internet Safety

CIFAS

Cloud Industry Forum (CILF)

Civil Court Users Association

Cloud Industry Legal Forum subgroup of the Cloud Industry Forum

Clyde and Co

Consumer Credit Association

Consumer Focus

Credit Services Association

Data Governance Forum

Dell

Direct Marketing Association

Duane Morris

Ebay

Employment Lawyers Association

Endemol

Energy Retail Association

Equifax

European Justice Forum

Experian

Facebook

Federation of Small Businesses

The Finance and Leasing Association (FLA)

Financial Services Authority (FSA)

Google

General Medical Council (GMC)

Great Ormond Street Hospital NHSFT (Legal Department)

Heinz College, Carnegie Mellon University

HSBC

The Health and Social Care Information Centre (HSCIC)

Hunton Williams

Internet Advertising Bureau (IAB)

Institute of Chartered Accountants in England and Wales (ICAEW)

Interactive Media in Retail Group (IMRG)

Information Commissioner's Office

Information Technology and Innovation Foundation

Institute of Practitioners in Advertising (IPA)

Institute of Professional Investigators

Intellect UK

International Association of Privacy Professionals

International Chamber of Commerce

International Financial Data Services

International Pharmaceutical Privacy Consortium (IPPC)

Information and Records Management Society (IRMS)

ISBA

Association of British Insurers

Janet (JNT Association)

Johnson and Johnson
Law Reform Committee of the Bar Council
Law Society
Leeds Council
Legal and General
Leicester City Council
Lewis Silkin
Licensing Executives Society
Mark King
Market Research Society (MRS)
Media Lawyers Association
Mercer
Microsoft
Midata
Milbank
Mobile Broadband Group
Mydex Data Services CIC
National Archives
National Assembly for Wales
NHS
Nokia Corporation
Open Digital Policy Association
Open Rights group
Pearson
Percy Crow Davies
PHG Foundation

Privacy Laws & Business Privacy Officers' Network

Professional Publishers Association (PPA)

Queen Mary, University of London

Regulatory Strategies Limited

Residential Landlords Association

Royal Mail

RSPB

SAI IT Consulting Ltd

Saint-Gobain Building Distribution Limited

Salesforce.com

Sidley Austin

Society for Computers and Law (SCL)

St James Place

Symantec

TalkTalk

Taylor Wessing

TechAmerica Europe

The CityUK

The Newspaper Society

The Number

Thomson Reuters

Transport for London

UK Cards Association

UK Council of Caldicott Guardians

Universities Scotland

US Chamber of Commerce

Venable LLP

Visa Europe

Wellcome Trust

West Yorkshire Police

Which

William Heath (representing several organisations including Mydex CIC)

Wolf Software Limited

Wragge & Co

WPP Group (submitted by Pinsent Masons)

Yuill and Kyle

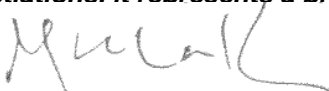
© Crown copyright 2012
Produced by the Ministry of Justice

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/ or email: psi@nationalarchives.gsi.gov.uk

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

Alternative format versions of this report are available on request from informationrights@justice.gsi.gov.uk

Regulation - Checklist for analysis on EU proposals

<p>Title of EU proposal: Regulation 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)</p> <p>Other departments/agencies with an interest: Department for Business, Innovation and Skills, Department for Culture, Media and Sport Information Commissioner's Office</p> <p>Date: 28th March 2012</p>	<p>Lead policy official: Ollie Simpson (ollie.simpson@justice.gsi.gov.uk) (020 3334 4556)</p> <p>Lead lawyer: Eleonor Duhs (eleonor.duhs@justice.gsi.gov.uk) (020 3334 4742)</p> <p>Lead economist: Chola Mukanga (chola.mukanga@justice.gsi.gov.uk) (020 3334 5233)</p> <p>Lead UKRep desk officer: Ben Hale (Ben.Hale@fco.gsi.gov.uk) (+32 (0) 2 287 8241)</p>
<p>What is the Commission proposing?</p> <p>The General Data Protection Regulation aims to update and replace the current data protection law, taking into account both the growth in the processing of personal data over the last fifteen years as well as a perceived lack of harmonisation in Member States which has produced barriers for data controllers in the internal market. It also aims to strengthen individuals' data protection rights by a series of new measures, including more stringent requirements for data controllers. The impacts of the proposal are identified below, with further detail set out at Annex A.</p> <p>Who are the main affected groups in UK?</p> <p>The Regulation will impact persons or organisations which process personal data ("data controllers" and "data processors"). This includes public sector organisations; private sector organisations and sole traders; and the third sector. It will also affect individuals whose personal data is being processed ("data subjects"); the Information Commissioner's Office (ICO); and the justice system.</p> <p>What are the main benefits to the UK?</p> <p>The benefits would largely fall to data subjects (individuals) from potential better safeguarding of their information; cheaper access to personal data; greater control over their personal data; and, strengthen access to judicial remedies. Business involved in cross border trade activity may also benefit from greater harmonisation of data rules; and abolition of the requirement to notify the ICO of processing activities.</p> <p>What are the main costs to the UK?</p> <p>The proposals would impose substantial costs on data controllers through increased burdens on businesses and third sector. This would include costs from new requirements relating to data protection officers, data breach notifications and high administrative sanctions. There may also be high costs associated with new and strengthened rights, such as the right to be forgotten, the right to data portability and the subject access requests. The Regulation may also impact international competitiveness due to more stringent requirements on international transfers. The ICO would incur significant costs in relation to the new obligations placed upon it.</p> <p>What is the overall impact?</p> <p>The overall impact is likely to be substantially negative. Though it is difficult to place a figure on the scale of net costs, the positive benefit to individuals of strengthened data rights are judged to be likely to be outweighed by negative impacts on small businesses, third sector, the ICO and wider justice system. These issues are explored in more detail at Annex A.</p> <p>Ministerial sign-off:</p> <p><i>I have read the analysis above of the potential impacts of this proposal and I am satisfied that, given the significance of the proposal, the time and evidence available, and the uncertainty of the outcome of negotiations, it represents a proportionate view of possible impacts.</i></p> <p>Signed by the responsible Minister:  Date: 24 April 2012</p>	

ANNEX A: ASSESSMENT OF IMPACTS

1. POLICY PROPOSAL

DESCRIPTION

1. The European Commission published new legislative proposals for data protection on 25 January. The proposals consist of a draft Regulation setting out a general EU framework for data protection and a draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. The draft Regulation will repeal and replace the 1995 Data Protection Directive, which is implemented into UK law by the Data Protection Act 1998.

PURPOSE

2. The draft Regulation aims to update and replace the current data protection law, taking into account both the growth in the processing of personal data in the last fifteen years (especially in the online world) as well as a perceived lack of harmonisation in Member States which has produced barriers for data controllers in the internal market. It also aims to strengthen individuals' data protection rights by a series of new measures, including more stringent requirements for data controllers.

AFFECTED GROUPS

3. The proposal will impact on persons or organisations which process personal data ('data controllers' and 'data processors'). This would include the following groups :
 - **Public sector data controllers:** includes the public sector including government departments, councils, and non-departmental public bodies.
 - **Private sector data controllers:** It will impact on the private sector, including large multinational corporations, small and medium enterprises, 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.
 - **Third sector:** it will impact on the third sector, including charities and voluntary organisations.
 - **Data subjects:** It will affect individuals whose personal data is being processed ('data subjects') by continuing to have their personal data protected by the law, with recourse to the data controller itself, a supervisory authority or the courts when their rights are infringed. They may also benefit from strengthened access, deletion and rectification rights.
4. The proposals would also impact on the **Information Commissioner's Office (ICO)**. Widening the scope of the ICO's responsibilities and powers may require more resources – for example undertaking prior authorisation, greater cooperation with supervisory authorities in other Member States, and the potential for more litigation involving the ICO.
5. There will also be an impact on the **justice system** if the proposals lead to more data protection cases in the courts.

6. The proposals will impact on UK citizens in other Member States and it will also apply to Gibraltar.

2. BASE CASE

7. The previous EU data protection instrument was the 1995 Data Protection Directive 95/46/EC, implemented into UK law by the Data Protection Act 1998 (DPA). The proposals for new instruments in the area of Data Protection came about as the 1995 Data Protection Directive is widely perceived to be out of date. Since 1995, there have been numerous technological developments, notably the expansion of the internet and the emergence of social media networks which has resulted in the processing of far higher volumes of personal data.

CURRENT LEGISLATION

8. The DPA regulates the obtaining, holding, use and disclosure of personal data and uses the term 'processing' to describe all these functions. It provides a framework to ensure that personal data are handled correctly. Organisations wishing to process personal data in the UK must comply with the DPA's eight data protection principles. Among other things, these require personal data to be processed fairly and lawfully, to be adequate, relevant and not excessive, accurate and kept up to date, obtained only for specified and lawful purposes, and not further processed (including disclosed to third parties) incompatibly with those purposes.
9. The Information Commissioner's Office (ICO) is the independent public body responsible for regulating and enforcing the DPA. The Information Commissioner has a range of powers available to him to enforce compliance with the DPA. Under the DPA, individuals ('data subjects') have the ability to exercise various rights around how their personal data is processed.

CURRENT TRENDS

10. The 2011 Post Implementation Review (PIR) of the DPA analysed the impact of compliance with the DPA. It found monetised costs for data controllers of around £53m per year and justice system costs of enforcing the DPA of around £1m. The PIR concluded that these figures are estimates and it was likely that the true cost of compliance is higher. The PIR also found non-monetised costs which included extra staff hired to ensure compliance with the DPA, costs for those who have received penalties, as well as impacts where the incorrect application of the DPA has stopped organisations sharing information.

3. IMPACT OF REGULATION

11. The assessment of the Regulation 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.
12. This checklist 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 the call for evidence. A table summarising these impacts can be found at the end of this document.

13. Based on the above criteria, the main policy areas assessed are:
- **One single law:** 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.
 - **Abolishing 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 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.
 - **Data protection officers:** 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:** The proposal sets out a requirement that data controllers must undertake a data protection impact assessment on data processing which presents specific risks.
 - **Strengthened subject access rights:** The Commission proposes making all subject access requests 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 the request.
 - **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.
 - **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.
 - **Complaints and judicial remedies:** The proposals include the right for organisations or bodies who represent individuals' data protection rights to seek a judicial remedy against either the supervisory authority or a data controller or processor.
 - **Supervisory authority role and powers:** The proposals include new 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.
 - **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.

ONE SINGLE LAW

Description

14. 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. Currently, Member States have implemented the 1995 Data Protection Directive by means of domestic legislation which is perceived to have brought about substantial differences between the different Member State legal frameworks.

Benefits of 'One Single Law'

Data controllers

15. The Commission states small and medium enterprises are refraining from offering online services in other Member States because they cannot afford the necessary legal expertise to ensure compliance with the local data protection rules. The Commission states that greater harmonisation will create a more predictable business environment, with a better functioning internal market as well as increased consumer confidence. Data controllers who operate in more than one Member State will also be able to deal with just one supervisory authority.

Individuals

16. Increased harmonisation may give individuals greater trust in how their personal data is used by organisations. They will also have more control over how their personal data is processed, and may find it easier to exercise their rights. As a result they may be more likely to use online services or to buy goods online.

Costs of 'One Single Law'

Data controllers

17. Harmonisation may result in increased costs if it generally increases the requirements (including administrative requirements) for data controllers, beyond those of the Data Protection Act 1998.
18. In particular, this may affect most those organisations who do not undertake large amounts of cross-border trading and so will be unlikely to receive many of the benefits of greater harmonisation. The proposals will not, however, achieve full harmonisation as there are still some individual Member State laws which data controllers will need to comply with.

Individuals

19. Individuals may face increased costs of goods and services if data controllers decide to pass the increased burdens onto them, for example charging for online services that were once available for free.

ABOLISHING THE NOTIFICATION SYSTEM

Description

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, set at £35 for organisations with fewer than 250 employees and a turnover of under £25.9m as well as public authorities with under 250 members of staff, and £500 for all organisations over these limits. The purpose of notification is to ensure transparency of processing through a register of data controllers which is publicly accessible. In 2010/11 the total amount raised by fees was £15m.

Benefits of Abolishing Notifications

Data controllers

20. The abolition of notifications would lead to two separate savings for data controllers :
 - **Notification fees:** If the notification requirement is abolished, data controllers will no longer have to pay £15m in fees and undertake the process of notification. However, the benefits may be limited if the UK could retain the flexibility to continue with some form of fee for data controllers to fund the data protection work of the ICO.
 - **Administrative savings:** The 2011 DPA Post Implementation Review estimated the cost of compliance with notification as £3m for data controllers, based on the time and resources taken to carry out the process of notification. There will also be a saving for data controllers who operate in several Member States as they will no longer have to undertake multiple notifications to each supervisory authority.

Regulator

21. There will also be a small saving in administration for the ICO who may no longer have to maintain a register or pursue non-compliant data controllers, as well as processing notifications and payments.

Costs of Abolishing Notifications

Regulator

22. Abolishing the notification system will result in a loss of £15m of fee income for the ICO. As this is the sole source of revenue for the ICO's data protection work there will need to be new arrangements for its funding.

DATA BREACH NOTIFICATIONS

Description

23. 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. Where the data breach is likely to adversely affect the data subject, the data controller must also notify them.

Benefits of Data Breach Notifications

Data controllers

24. If data controllers are required to notify breaches, they may take action to ensure fewer data breaches, such as implementing more robust security measures, thus avoiding further enforcement action or the cost of data breaches. The requirement may also result in fewer breaches through a deterrent effect. In its 2010 Information Security Breaches Survey, carried out by PwC, InfoSecurity Europe put the average business cost of the worst security breach at between £27,500 and £55,000 for a small organisation and between £280,000 and £690,000 for a large organisation. These costs include, among other things, investigating and responding to an incident, financial loss due to fraud, and damage to reputation. Successful ICO enforcement action with regard to breaches may also have a deterrent effect on data controllers.

Individuals

25. Individuals may benefit from less risk of fraudulent use of their personal data. The 2011 e-Privacy IA estimated that if notification led to a 0.1% fall in the annual cost of identity theft, consumers would benefit by around £1.4m to £1.7m¹. Individuals may also benefit from less risk of distress or material damage when their personal data is lost or stolen.

Regulator

26. An increase in data breaches notified to the ICO will give it more information to take enforcement action against data controllers who have breached the legal framework.

Costs of Data Breach Notifications

Data controllers

27. The number of data breaches reported to the ICO has been increasing over the last five years, and in 2010/11 there were 603 breaches reported. However, only public sector organisations are required do so, so the total number of breaches is likely to be higher. The 2010 Symantec/Ponemon Institute study 'UK Cost of a Data Breach', based on a survey of 38 companies, found the cost of a data breach for UK organisations to be £71 per record, including £6 for notification costs for data controllers. It found that companies on average paid £172,000 per breach for notification costs.

¹ This is based on the Detica/Cabinet Office report 'The Cost of Cyber Crime' (February 2011) which estimated the economic cost of online identity theft at around £1.7 billion per year and stated £1.4 billion was lost annually due to online scams.

28. There is an existing requirement for electronic communication service providers to report breaches under the 2009 e-Privacy Directive. The cost of compliance in the 2011 Impact Assessment for the e-Privacy Directive was estimated at £210,000 per data breach. However it noted that there would be no additional costs if the organisation is already notifying the ICO of such breaches.
29. There will be costs for data controllers in notifying the ICO and individuals of breaches. At the moment, under current Cabinet Office guidance, government departments and NHS bodies must report data breaches to the ICO. This means the impact of mandatory data breach notifications will be limited for public sector organisations unless they experience a higher level of breaches. They will however still need to notify individuals. In 2010/11, 64% of breaches (388) reported to the ICO were from public sector data controllers.
30. Some private sector data controllers will already notify individuals as a matter of practice, but it is not clear how widespread this is. In 2010/11, 31% of breaches reported to the ICO were from private sector data controllers. While it is hard to estimate the number of breaches that will be notified, given that the proposals specify all breaches (bar those where the data is encrypted) there are also likely to be a significant number of minor breaches which are not reported to the ICO or notified to individuals. Therefore, taking the 2010/11 figures for breaches reported to the ICO as a base, if there are the same number unreported, this would equate to an additional notification cost of £104m (603 x £172,000).
31. If the ICO receives more reports of data breaches from data controllers, it will have more evidence on which to potentially take enforcement action. Data controllers will therefore face additional enforcement costs if the ICO decides to take action against them. Data controllers may also take an overly cautious approach to breach notification, and spend time and resources on reporting incidents which are beyond the legal requirement.

Individuals

32. Individuals may suffer from 'notification fatigue' if the threshold set for data controllers to notify them results in a large number of notifications, and ignore these. They may also suffer from increased distress if they cannot take any appropriate action to mitigate the impact of the additional notified breaches. They will also be aware of breaches which affect them and be able to take appropriate action to minimise the risk of damage.

Regulator

33. The requirement is likely to result in more notifications to the ICO. There will therefore be a resource cost in recording and handling these. There are also likely to be costs for the ICO if it takes more enforcement action on the basis of the increased numbers of notified data breaches.

Other Groups

34. There may also be costs for the justice system where individuals decide to pursue individual breaches through the courts. It is hard to quantify the number of cases at present.

DATA PROTECTION OFFICERS

Description

35. 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. The proposal also sets out a list of tasks for data protection officers and the requirement that these must be performed independently.

Benefits of Data Protection Officers

Data controllers

36. Employing data protection officers may potentially aid compliance with the legal framework and fewer infringements, leading to fewer data breaches, increase in customer confidence and less risk of enforcement action and sanctions from the ICO.
37. It will, however, be difficult to quantify the benefits from employing data protection officers and to separate these benefits from the impact of other new requirements in the Regulation or separate factors, for both individuals and data controllers.

Costs of Data Protection Officers

Data controllers

38. There will be costs for data controllers from employing a data protection officer and providing them with appropriate resources. The proposal sets out that this should include 'staff, equipment, premises and any other resources necessary'.
39. In 2010/11, around 5,900² data controllers notified the ICO as large organisations (i.e. over 250 employees and have a turnover of over £25.9m employees). If we estimate that cost of employing a data protection officer as £50,000 a year this represents an overall monetary cost of £295m. However, it is likely that larger organisations and public bodies will already have someone undertaking a similar role, so it will be difficult at present to accurately quantify this cost. If we assume that 50% of organisations will already have a member of staff fulfilling this role, the additional cost will be £147m per year. These costs are far higher than the Commission's estimated costs to businesses of around €320m per year across all Member States.
40. The costs are likely to be greater for small public bodies (such as arms-length bodies) and small firms who undertake large amounts of data processing, such as hi-tech start-ups and medical research organisations, where the annual cost of £50,000 would be a considerable burden.
41. In their response to the 2012 Call for Evidence, the CBI stated:
"The requirement for all organisations with more than 250 employees to appoint a Data Protection Officer (DPO) who must then be employed for two full years is similarly costly and disproportionate, especially for organisations where data processing only forms a tangential part of their overall activities. Recent job

² Based on 2010/11 notification fee income of £2,961,000 for Tier 2 fees at £500 per data controller.

advertisements typically show that a qualified DPO in the South-East of England could earn anything between £30,000 and £75,000 per annum.”

DATA PROTECTION IMPACT ASSESSMENTS

Description

42. The proposal sets out a requirement that data controllers must undertake a data protection impact assessment on data processing which presents specific risks (such as information on an individual's sex life, health, race and ethnic origin, or the monitoring of publicly accessible areas using CCTV.)

Benefits of Data Protection Impact Assessments

Data controllers

43. As per data protection officers, mandatory data protection impact assessments may aid compliance with the legal framework, potentially leading to fewer data breaches, improve customer confidence and less risk of enforcement action and sanctions from the ICO. However, it is impossible to deduce the extent of these benefits and the extent to which they would be distinct to the benefits of the general requirements in the Regulation.

Costs of Data Protection Impact Assessments

Data controllers

44. There will be a cost for data controllers in the time and resources taken to undertake a data protection impact assessment. This is difficult to quantify. Currently government departments are required to consider and undertake data protection impact assessments for all new proposals so the additional impact of the new requirement should be less onerous on government departments. Considering other data controllers in both the private and public sector, it is unclear how many of them are undertaking similar work – the ICO has produced and marketed comprehensive guidance on data protection impact assessments to data controllers.
45. The Commission estimate that the cost of undertaking a data protection impact assessment may cost €14,000 (e.g. marketing firm) or €34,500 (e.g. for location based services) or as much as €149,000 (for large multi-national firms). If we take the estimate of 5,900 data controllers and assume that half of these will need to undertake an assessment once a year, split evenly between the three examples provided by the Commission, the cost will be £163m³ per year.
46. For example, in their response to the 2012 Call for Evidence, Leeds City Council set out some of the impacts of data protection impact assessments.
“These provisions represent significant additional burdens for local authority data controllers. In particular, authorities are likely to carry out processing falling 2.(a)-(c), and will certainly process ‘personal data in large scale filing systems on children’, and therefore will be required to carry out a full, formal impact assessment of their relevant processing activities. In addition, where such an assessment indicates their operations are likely to present ‘a high degree of

³ Worked out as 5,900/6 = 983 data controllers; multiplied by 14,000, 35,500 and 149,000, equals €195m, which is £163m.

specific risks’, (and it is anticipated that in larger authorities, the very nature and scope of processing activities as regards children means such risks are unavoidable), there is a requirement on the controller to consult the supervisory authority prior to processing, with a power for the supervisory authority to ‘prohibit’ the intended processing. It is considered these requirements will use a disproportionate amount of resource, and will build in delays to processing activities. In addition, where processing is being carried out by a public authority in the discharge of its statutory functions, there should be no power for the supervisory authority to ‘prohibit’ processing.”

Regulator

47. The ICO will have to be consulted on some data protection impact assessments where they indicate that processing is likely to present a high degree of specific risks, and may require additional staff. Based on the estimate above, the ICO will need to authorise around 5,250 assessments every year.

STRENGTHENED SUBJECT ACCESS RIGHTS

Description

48. The Commission proposes making all subject access requests free of charge. It also proposes widening the amount of information that data controllers must provide (including the amount of time the data will be stored for), requiring that it must be supplied in an electronic format where the requester has made the request electronically, and setting a time limit of a month to comply with the request.

Benefits of Strengthened Subject Access Rights

Individuals

49. There will be a benefit for individuals of not having to pay £10 per request. It may encourage more people to exercise their right to subject access, (including the ability to correct their personal data if appropriate) as some may have been deterred by the current fee system. This could mean, for example, that better credit decisions are made about individuals, although it is notable that only a small proportion of challenged credit records result in an actual amendment, after investigation. Individuals should also receive their information quicker than before.

Costs of Strengthened Subject Access Rights

Data controllers

50. The 2011 Post Implementation Review of the Data Protection Act found the overall cost of compliance with SARs to be around £50m per year for the UK as a whole. In the 2010 Call for Evidence respondents believed that this figure significantly underestimated the cost of compliance. They generally estimated a cost of between £100 and £500 per SAR, and said the volumes of requests had increased in recent years. There were also particularly high volumes reported by some public sector data controllers. Currently data controllers in the UK may charge a fee, which is set at £10 for most requests, £2 for information for requests to credit reference agencies relating to an individual's financial standing, and up to £50 for some educational and medical records.

51. One cost of free SARs will be the loss of fee income for data controllers. The fee currently does not defray totally the cost of compliance, but its loss will represent a cost to data controllers. There is also the cost of providing more information, such as the time for which the data will be stored. This cost is difficult to quantify. One further cost will be a potential rise in the numbers of SARs. The current fee structure is designed to deter frivolous requests and so if this barrier no longer exists, data controllers are likely to receive more requests. There will also be a cost of having to provide the information more quickly – the current time limit in the UK is 40 days, compared to the Commission’s proposal of a month.
52. For example, in their response to the 2012 Call for Evidence, the Association of British Insurers also considered the impact of free SARs.

“The proposed timescales fail to take account of the size and diverse nature of organisations, and the different issues experienced in relation to the recovery of data from other organisations within the group or associated organisations. The proposals also fail to take into account the complexity of some SARs, be it in terms of the volume or nature of information requested. For example:

- *An insurer receives a SAR from a customer who has held a life insurance policy with the firm for 20 years. They request „all data” relating to them.*
- *An employee makes a SAR which requires other employee email accounts to be searched for their personal data.*
- *An employee makes a SAR for their HR file which is very large. The firm needs to consult with the individual's psychiatrist to ensure that disclosure would not be detrimental to their health.”*

Regulator

53. Any increase in the number of subject access requests may also lead to more complaints to the ICO where individuals are not happy with the outcome of their request or where it is refused. The ICO will therefore need to dedicate more resources to handling this type of casework.

DATA PORTABILITY

Description

54. 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. It also allows data subjects, in some circumstances, to transfer data from one automated processing system to and into another, without being prevented from doing so by the data controller.

Benefits of Data Portability

Data controllers

55. There are existing proposals for similar work being undertaken by the Department of Business, Industry and Skills' 'midata' initiative. This aims to encourage organisations to allow people to view, access and use their personal and transaction data in a way that is portable and safe. It is, however, taking place on a non-mandatory basis. There may be benefits for data controllers if the new proposals encourage the rise of new information services, promoting economic growth. There may be a benefit for small businesses if individuals find it easier to move to them rather than large service providers.

Individuals

56. Individuals will have greater freedom of choice and will find it easier to move their personal data between competitors and secure better value for money. It may also give individuals the ability to make better decisions about a wide range of products and services.

Costs of Data Portability

Data controllers

57. There will be a cost to all data controllers of passing personal data to data subjects and/or competitors, including data cleansing and changes to IT systems. It is difficult to estimate costs as this depends on the particular circumstance of each data controller. There will also be costs if confidential trade information is passed to competitors under this new right. However, such costs will be mitigated if data controllers are already undertaking this work, for example, through providing online account services for bills, statements or other information. The cost of providing personal data as part of the right to data portability may be significantly lower than providing paper copies under the right to subject access.
58. In their response to the 2012 Call for Evidence, Microsoft set out some of the impacts of the right to data portability.

"Microsoft absolutely supports giving individuals more control over their data – increased data mobility is not only good for users, it is also good for business and the overall ecosystem. But the Regulation should recognise the technical reality that the ability to export data does not necessarily mean that such data can be used "as is" in other services... the successful transfer of data from one service to another is not a simple proposition – and mandating a single format for data transfer will require technology providers to change other aspects of their products and services which may result in less functionality, less diversity and a worse overall user experience."

Regulator

59. There may be enforcement costs for the supervisory authority if there are disputes between individuals and data controllers, including more complaints handling.

RIGHT TO BE FORGOTTEN

Description

60. The proposal sets out a new right to be forgotten, including the right to obtain erasure of personal data relating to them and the abstention from further dissemination of such data. This builds upon the existing deletion rights in the DPA and the principle that data controller should not process personal data for longer than is necessary. It would have a specific impact on removal of information retained in an online setting, especially that data which has been made widely available by one website to many others.

Benefits of Right to Be Forgotten

Individuals

61. Individuals may benefit from strengthened control of their personal data through the new rights which lessens the risk of harm or discrimination to them on the basis of incorrect or out-of-date personal data. This could occur, for example, through employers searching for embarrassing photos of potential employees.

Costs of Right to Be Forgotten

Data controllers

62. There will be a cost for data controllers to comply with the new requirements including time spent on requests and changes to IT systems. This will impact heavily on data controllers who operate internet search engines. Without sufficient exemptions (which could be put in place by Member States), there could also be impacts on the lending sector and any other organisations which rely on historic consumer data to make decisions – which could lead to higher costs of credit for some individuals. While there are exemptions for research and freedom of expression purposes, there will still be an impact in the need to explain this to individuals. If we assume that the cost for a data controller to update their systems to comply with the new requirement is between £2,000 (for a small business) and £200,000 (for a large company), if 50% of data controllers need to make such changes, the estimated cost will be £932m⁴.
63. For example, in their response to the 2012 Call for Evidence, WPP considered the impact of the right to be forgotten.

“WPP companies expect to spend £2 billion on Google ads alone in 2012 and to increase spending across a wide range of hosted platforms including Facebook and Twitter. WPP companies also rely extensively on the use of data lists to deliver their entire core of marketing services, whether they are compiled by WPP agencies, clients, data collection companies or UK government agencies. The right to be forgotten and its potentially more onerous administrative requirements as well as the increased uncertainty it creates as to whether data list creators will be able to guarantee the use of the data to their clients, may place the existing business models under untenable strain.”

⁴ Calculated using the ICO's 2010/11 fee income from data controllers, which indicates an estimated 340,376 data controllers paying a £35 fee and 5,922 paying a £500 fee.

Regulator

64. There will also be enforcement costs for the ICO in ensuring that organisations uphold these rights, given that there may be a high demand for the right in the first years of implementation, with subsequent costs for the justice system including the courts.

Other Groups

65. There may be justice system costs if the new requirement leads to more individuals seeking redress through the courts.

ADMINISTRATIVE SANCTIONS

Description

66. 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 €1,000,000 or 2% of an enterprise's annual worldwide turnover, which could be as high as several hundred million euros for the largest enterprises.

Benefits of Administrative Sanctions

Data controllers

67. Administrative sanctions may lead to better compliance with data protection requirements and therefore fewer infringements such as personal data breaches. The ICO already has the power to issue civil monetary penalties up to £500,000 and issued four penalties to the value of £310,000 in 2010/11 and ten penalties to the value of £861,000 in 2011/12. However, it is difficult to assess whether there is a substantial link between better compliance with the DPA and the introduction of the penalties.

Other groups

68. If administrative sanctions are paid into the Consolidated Fund (as per civil monetary penalties) there may be an increase in revenue for the Government. This would however be limited if the new sanctions are an effective deterrent and are rarely issued.

Costs of Administrative Sanctions

Data controllers

69. As the criteria for issuing sanctions in the proposals is wider than the DPA, it is likely that there will be more sanctions than at present. This will result in further costs for data controllers especially given the threshold of 2% of annual global turnover.

In their response to the 2012 Call for Evidence, the CBI stated:

“For a large multinational organisation, such as a major bank or insurer, 2% of global turnover could represent hundreds of millions of pounds. HSBC, for instance had global revenues of \$99bn in 2010, or around £63bn. Thus a 2% fine, if applied in full, could potentially cost the company in the order of £1.2bn.”

Regulator

70. There may be a burden on the ICO if it has to devote more time to issuing administrative sanctions and other penalties. The Impact Assessment for the introduction of civil monetary penalties estimated the administrative cost to the ICO of serving such penalties in 2009 at £17,500 per year. The proposed new sanctions would go further than the criteria for civil monetary penalties, and appear to *require* supervisory authorities to serve sanctions on data controllers and processors, so it is likely that the ICO will need to spend more resources in deciding when and how to serve these new sanctions. It is, however, difficult to quantify how often the sanctions will be applied, given that they are covering a far wider range of infringements than at present.

Other Groups

71. There may also be additional costs for the justice system, if more data controllers appeal against the proposed sanctions. However, this will depend on the extent to which these exceed the current number of civil monetary penalties handed down (again, noting the potential requirement for the ICO to serve penalties where there has been a breach of certain of the Regulation's requirements). It also depends on the extent to which such costs are recoverable from existing court fee structures.

COMPLAINTS AND JUDICIAL REMEDIES

Description

72. The proposals include the right for organisations or bodies who represent individuals' data protection rights to seek a judicial remedy against either the supervisory authority or a data controller or processor. Data controllers will also have the right to seek a judicial remedy against the supervisory authority. The aim is to make it easier to seek legal redress where appropriate.

Benefits of Complaints and Judicial Remedies

Data controllers

73. There may be benefits for data controllers from the ability to seek a judicial remedy against the decision of the ICO. This could also result indirectly in more transparency in the ICO's decision-making, which could give data controllers greater insight into its regulatory strategy.

Individuals

74. Individuals could receive quicker or more effective redress for the damage caused by infringements of the Regulation. There may be fewer infringements of the legislation by data controllers if it is easier for individuals to obtain redress.

Costs of Complaints and Judicial Remedies

Data controllers

75. There may be a rise in litigation among data controllers, with increased legal costs for either taking cases or defending them. Data controllers may be more cautious in how they undertake their data processing and incur extra costs through a 'belt and braces' approach.

Individuals

76. Individuals will face new legal costs if they decide to enforce their rights by way of a judicial remedy rather than using the current means of either making a complaint to the ICO or resolving the complaint with the data controller – both these means are free of charge to individuals.

Regulator

77. There will also be costs for the supervisory authority, if they are more likely to be challenged on their decisions or the nature of their processing. It is difficult to quantify costs without understanding the total number of extra cases which are likely.

Other Groups

78. The proposal may lead to more court proceedings, with associated costs on the justice system. It is, however, difficult to quantify the number of cases. The additional cost also depends on the extent to which such costs are recoverable from existing court fee structures.

CHANGES TO SUPERVISORY AUTHORITY ROLE AND POWERS

Description

79. The proposals include new requirements for supervisory authorities to provide mutual assistance to each other in Member States. This is intended to ensure that the Regulation is implemented and applied in a consistent manner. There are also proposals which specify that Member States shall ensure that supervisory authorities have adequate resources to carry out its duties.

Benefits of Changes to Supervisory Authority Role and Powers

Data controllers

80. Data controllers may benefit from legal certainty if they know that they will face the same regulatory treatment in different Member States as a result of the harmonisation of powers of supervisory authorities as set out in the proposal.

Individuals

81. Individuals may benefit from increased confidence that cross-border issues are being handled effectively and that with additional resources, the ICO is able to

take a more vigilant approach and prevent infringements of the legal framework.

Costs of Changes To Supervisory Authority Role And Powers

Regulator

82. The ICO will need more resources to undertake its increased responsibilities, and this will either have to come directly from data controllers in the form of fees, or indirectly from individuals and data controllers in the form of increased public expenditure. The ICO will also have to take on extra work to support requests from other supervisory authorities. It is difficult to estimate the extent of this work but the European Commission suggest this will mean an additional two or three members of staff for each supervisory authority.

CHANGES TO INTERNATIONAL TRANSFERS

Description

83. 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. The derogations which data controllers can use have also been changed, and are more restrictive than the current situation. It is also important to consider that the volume and type of transfers has changed dramatically since 1995.

Benefits of Changes to International Transfers

Data controllers

84. There may be more legal certainty (and fewer costs) if data controllers can rely more on adequacy decisions and binding corporate rules, rather than having to deduce the level of data protection in a non-EEA country themselves. It is, however, difficult to quantify this benefit as there is little evidence available of the numbers of transfers which take place, or the sectors involved.

Individuals

85. Individuals may benefit from less risk that their data is misused when it transferred to a third country if the new requirements are effective. They may have more confidence in organisations which process their personal data overseas.

Costs of Changes to International Transfers

Data controllers

86. Data controllers may have to rely on more lengthy methods of authorisation if they can no longer rely on the derogations, thus incurring more legal costs if they choose to use standard data protection clauses or seek authorisation from the ICO.

87. There may also be costs for data controllers (and subsequently to individuals) if they decide not to process data abroad because of the cumbersome nature of the authorisation methods, and therefore have to do so in the EU, at a higher cost. There are likely to be particular impacts on the use of cloud computing, especially if this is restricted by the new proposals, leading to higher costs for data controllers.

In their response to the 2012 Call for Evidence, Symantec considered the impact of changes to the system of international transfers.

“The requirement for contractual clauses to be authorised by authorities prior to engaging a sub-processor is seen as potentially over burdensome. Not only would it introduce additional red tape in a time when the Commission is seeking to reduce the burden on businesses but it could also have a potentially disruptive impact particularly on the cloud computing model. Cloud computing makes effective, yet low cost, protection of personal data possible for small and medium companies that without such capabilities being on offer may suffer significant breaches as a result of a lack of resources to employ security expertise. However, if this requirement in Article 42 remains it could significantly disrupt the future development of cloud computing in Europe, which sits at the very heart of the Commission’s Digital Agenda.”

Regulator

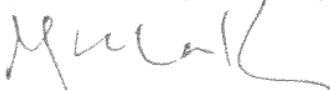
88. There will be additional costs for the ICO if it has to undertake more prior checking of international transfers of personal data.

4. SUMMARY OF IMPACTS

Table 1: Benefits of Selected Proposals			
	Data controllers	Individuals	ICO & Other
One Single Law	Legal certainty, fewer burdens in complying with rules	Increased consumer confidence in data protection across MS	n/a
Abolishing Notifications	Potential benefit of £18m from administrative burden & fees	n/a	Saving from no longer having to administer the notification process
Data Breach Notifications	Fewer data breaches and their associated costs	Less abuse of their personal data through data breaches	More information with which the ICO may take enforcement action
Compliance (DPOs / DPIAs)		Fewer infringements of individuals' rights	
Strengthened subject access rights		Easier to obtain subject access request	
Data Portability	Economic benefit of new information services fuelled by portability right	Greater freedom of choice	
Right to be Forgotten	n/a	Strengthened control of personal data	
Sanctions		Fewer infringements of individuals' rights	
Complaints and judicial remedies		More effective redress for infringements	
DPA role powers	Legal certainty: can expect same regulation in all Member States	Increased consumer confidence in data protection across MS	
International Transfers	Increased legal certainty	Less risk of infringements of individuals' rights outside of EEA	

Table 2: Costs of Selected Proposals			
	Data controllers	Individuals	ICO & Other
One Single Law	Increased compliance costs if the new harmonised requirements go beyond existing data protection rules	Potential for increased costs of good and services if data controllers pass on increased compliance costs to them	n/a
Abolishing Notifications	n/a	Loss of transparency of data controller's data processing activities	Loss of income, will require new funding arrangements
Data Breach Notifications	Notification costs of all data breaches – estimated at £104m	Individuals may grow tired of receiving notifications and take no interest in them	Increased cases for the justice system
Compliance (DPOs / DPIAs)	Cost of employing data protection officers estimated at £131m		Will need to authorise some data protection impact assessments
Strengthened subject access rights	Cost of handling more subject access requests and loss of fee income		More complaints from increased numbers of subject access requests
Data Portability	Cost of changes to IT systems and services		More complaints and enforcement costs if right is not complied with
Right to be Forgotten	Cost of changes to IT systems and services		More complaints and enforcement costs if right is not complied with Increased cases for the justice system
Sanctions	More likelihood of sanctions and higher value sanctions		Burden on the ICO if it has to spend more time enforcing sanctions Increase cases (including appeals) for the justice system
Complaints and judicial remedies	Increased legal costs in either taking on cases or defending them		Increased legal costs from defending its decisions Increased cases for the justice system
Supervisory authority role and powers	May take a more cautious approach to data protection, incurring additional costs		Will require more resources to perform additional responsibilities
International Transfers	Additional costs for data controllers from complying with lengthy new requirements		Costs of having to undertake more prior checking of international transfers

Directive - Checklist for analysis on EU proposals

<p>Title of EU proposal: Directive 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.</p> <p>Lead department: Ministry of Justice</p> <p>Other departments/agencies with an interest: Home Office, Police, Serious Organised Crime Agency (SOCA), Information Commissioner's Office (ICO), UK Border Agency (UKBA), Security Services</p> <p>Date: 28 March 2012</p>	<p>Lead policy official: John Bowman (john.bowman@justice.gsi.gov.uk) (020 3334 3150)</p> <p>Lead lawyer: Anne-Marie Donnelly (anne-marie.donnelly@justice.gsi.gov.uk) (020 3334 4740)</p> <p>Lead economist: Chola Mukanga (chola.mukanga@justice.gsi.gov.uk) (020 3334 5233)</p> <p>Lead UKRep desk officer: Ben Hale (Ben.Hale@fco.gsi.gov.uk) (+32 (0) 2 287 8241)</p>
<p>What is the Commission proposing?</p> <p>The European Commission has proposed a draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties. The Directive will repeal and replace the EU's 2008 Data Protection Framework Decision (DPFD). The impacts of the proposal are identified below, with further detail set out at Annex A.</p> <p>Who are the main affected groups in UK?</p> <p>The Directive proposal will impact on any public authority which processes personal data with regards to criminal offences or penalties. These include all Criminal Justice System (CJS) agencies e.g. Police, Courts. The proposals also affect the Information Commissioner's Office (ICO) as the UK information Regulator.</p> <p>What are the main benefits to the UK?</p> <p>The benefits would largely fall to data subjects (individuals) from potential better safeguarding on their information leading to fewer data breaches. There may also be wider benefits from society through improved security due to the potential for better sharing of data related to criminal offences that will increase the security of the UK.</p> <p>What are the main costs to the UK?</p> <p>The proposals would impose substantial costs which would largely fall on criminal justice agencies and the ICO due to increase in resource burden on these groups as they devote staff and other resources to fulfil these new obligations. It is also possible that there will be a cost to data subjects if these new obligations reduce the efficiency and effectiveness of data processing, which could impact on how well citizens' data protection rights are protected.</p> <p>What is the overall impact?</p> <p>The overall impact is likely to be substantially negative, though it is difficult to place a number on it. The proposals are likely to impose new costs on criminal justice system agencies and the ICO. Though some measures are designed to aid good practice, many of the new obligations appear disproportionate and unnecessary leading to an overall negative outcome. These issues are explored in more detail at Annex A.</p> <p>Ministerial sign-off:</p> <p><i>I have read the analysis above of the potential impacts of this proposal and I am satisfied that, given the significance of the proposal, the time and evidence available, and the uncertainty of the outcome of negotiations, it represents a proportionate view of possible impacts.</i></p> <p>Signed by the responsible Minister:  Date: 24 April 2012</p>	

ANNEX A: ASSESSMENT OF IMPACTS

1. POLICY PROPOSAL

DESCRIPTION

1. The European Commission published new legislative proposals for data protection on 25 January. The proposals consist of a draft Regulation setting out a general EU framework for data protection and a draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities with the execution of criminal penalties. The draft Directive will repeal and replace the EU's 2008 Data Protection Framework Decision (DPFD).
2. This checklist considers the potential impact of the Directive on the UK. In doing so, it focusses on the impact of several specific changes, taking into account the evidence currently available.

PURPOSE

3. Rapid technological and information exchange developments in recent years necessitate a modern data protection legal framework. The Directive seeks to ensure a high level of personal data protection for individuals across the EU in the context of EU policies for law enforcement and crime prevention. The specific nature of data processing in the field of police and judicial cooperation necessitate an instrument devoted to that purpose, based on Article 16 TFEU, which gives the EU the legal ability to legislate on personal data protection in order to ensure that everyone has the right to the protection of personal data concerning them.

AFFECTED GROUPS

4. The proposal will impact on public authorities ("competent authorities") that processes personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. However, a competent authority that is processing data that does not relate to criminal offences or penalties will not be covered by this Directive; instead the Regulation will apply, even if their usual business would be covered by this proposal. Competent authorities include all Criminal Justice System (CJS) agencies, including the Police, Crown Prosecution Service, HMCTS, Probation, Youth Offending Services, Prisons, agencies with powers of prosecution and the judiciary.
5. It is likely to affect the Police and other law enforcement authorities with regard to the processing of personal data. In particular, the scope of the legislation is being extended to include internal/domestic processing: all data transfers between domestic UK police forces (for example, data sent from the Metropolitan Police to South Yorkshire Police). This was previously not covered by the 2008 DPFD.
6. Suspects, defendants, victims, witnesses will also be affected by the proposals by continuing to have their personal data protected by the law, with recourse to either a supervisory authority or the courts when their rights are infringed. This proposal therefore impacts on the civil liberties of citizens in general.

7. The Information Commissioner's Office (ICO), the UK's supervisory authority that regulates *inter alia* data protection policy, will also be affected. There is a widening of the powers of the ICO and more areas where it will need to regulate and therefore both its scope and resource requirements will be increased.
8. The proposed Directive will apply to the entire of the United Kingdom (England, Scotland, Wales and Northern Ireland). The Directive also applies to Gibraltar in the same way as it does to the UK.

2. BASE CASE

9. Assessment of the proposed Directive on affected groups and nationally has been undertaken against the base case scenario of existing data protection legislation. Presently, data protection in the UK is provided for in the UK Data Protection Act (DPA) 1998. This transposed Directive 95/46/EC, which did not cover data processing in the context of police and judicial cooperation, into UK law. In adopting the DPA, however, the UK did extend some of its measures to cover CJS agencies, in this regard going beyond the minimum scope required in the Directive. The new Directive, as proposed, goes beyond what the UK has implemented, however.
10. Furthermore, the Data Protection Framework Decision (2008/977/JHA) was adopted in 2008, which provided data protection safeguard obligations in the context of police and judicial cooperation. It is this Decision that the proposed Directive seeks to repeal and replace.
11. The Directive looks to increase data protection safeguards compared to the DPF, which was very short, principles-based and high level. By contrast, the proposed Directive is longer, more detailed and more prescriptive. It places various new obligations on data processors that were not seen in the DPF. However, some of these obligations, though absent from the DPF, exist anyway within the UK Data Protection Act, as this was passed with some data processing within the context of police and judicial cooperation within its scope.

3. IMPACT OF DIRECTIVE

12. The assessment of the Directive has focused on addressing the impacts relative to the base case, focusing particularly on the impact on the criminal justice system; individuals; and, the information commissioner.
13. There has been some difficulty in quantifying some of the impacts, namely due to a lack of existing research or figures in these areas (most research on the impacts of data protection legislation have focussed on businesses). However, where possible, specific costing or estimates have been given.
14. In assessing the impact of the Directive, it has been necessary to devise criteria to guide the assessment given the detailed and varied nature of the proposals. This checklist has focused on those policies which are likely to have a relatively significant impact (positive or negative) on the UK; may be of important public debate; and areas raised in the call for evidence. In particular, the assessment focuses on those parts of the proposed Directive that suggest an increase in costs on CJS agencies or the ICO or the potential to adversely impact their operational capacity or effectiveness.
15. It is important to note, however, that Article 6a of the UK and Ireland's Title V Protocol (Protocol 21 TFEU) is likely to mean that there is a limited application of the Directive to the UK (and Ireland). Although no final position has been

agreed with the Commission, current UK legal opinion of Article 6a of the Protocol means that the Directive will only apply in instances where data processing is being carried out pursuant to an EU measure that binds the UK. This necessarily excludes internal processing from applying to the UK if this legal opinion is accepted. It also means that any rights exercised in regards to internally-processed data, such as rights of access to Police data, will not apply to the UK.

16. Based on the above criteria, the main policy areas assessed are :
- **Internal processing:** the scope of the Directive will, for the first time, cover processing carried out within a Member State, in addition to the present scope that covers international transfers where data emanates from within the EU.
 - **Free subject access requests:** data subjects will be able to make subject access requests free of charge, thereby eliminating the current ability of data controllers to charge a fee of up to £10 per request.
 - **Rights to erasure and rectification:** there will be expanded rights for data subjects to seek the erasure or rectification of their personal data held by data controllers.
 - **Data breach notifications:** data controllers will be under greater obligations regarding informing the ICO and data subjects in case of a personal data breach.
 - **Data protection officers:** a new obligation exists for data controllers to appoint data protection officers to oversee their compliance with data protection rules
 - **Documentation and records:** there is a new obligation for data controllers and processors to keep documentation and records regarding their processing of personal data
 - **Prior consultation:** a new obligation that requires data controllers and processors to consult with the ICO before using new automatic filing systems where special categories of data are to be processed or where the type of processing holds specified risks.
 - **Rules for International transfers:** new rules are laid out in the Directive regarding the transfer of personal data to countries outside of the EEA, adding specific requirements that must be met in order for the transfer to be permitted.

INTERNAL PROCESSING

Description

17. The current scope of the Data Protection Framework Decision is limited to cross-border processing activities. This will be widened in the current Directive proposal to include internal processing: that processing of personal data carried out between two CJS agencies, such as two separate UK Police forces. This will mean that a much greater quantity of operations involving personal data carried out by CJS agencies will be within the scope of the Directive.

Benefits of Internal Processing

Criminal Justice System

18. An increase of the scope of data protection rules to cover internally processed data may act as an assurance that the UK is complying with data protection rules internally in regards to criminal offences and penalties. It may re-assure other states that our data protection safeguards are adequate. This could mean that other member states may be content to share data with our CJS agencies. This ease of data sharing may reduce costs for CJS agencies if it would otherwise have cost them resources to pursue data from other states that they were less content to share. For example, sharing under the European Investigation Order, which enables the Crown Prosecution Service to use information held by its EU counterparts in UK trials, will almost certainly use the Directive as its data protection basis. By complying with internal processing rules, data will be shared between Member States may be more content to share this information freely.

Individuals

19. Individuals whose data is processed by competent authorities internally may be assured the higher level of data protection afforded by the Directive. This may help to reduce the frequency of data breaches or other unauthorised actions that have a negative impact on individuals if it creates a better framework for the protection of personal data.

Costs of Internal Processing

Police

20. The Police forces may be particularly impacted by this proposal as it is likely that there will be a great quantity of data that is processed between the UK's fifty-two territorial police forces, in particular where a criminal investigation is being conducted over a wide geographical area.

Other Criminal Justice System Agencies

21. The new requirement in the proposals for processing to apply to internal processing is likely to lead to additional administrative burdens when exchanging and processing information between criminal justice agencies in the process of crime prevention, public protection and bringing offenders to justice. It is likely that the widening of the scope would cover a lot more day-to-day data processing and therefore add burdens to quite a large area of CJS work as the Directive's rules will apply to a greater proportion of the data processing that they carry out.
22. The impact of this extension of scope must be read alongside the other economic impacts that the new Directive may have as they will need to be applied additionally to instances of domestic data processing and not just the less common occurrence of data processing between EU Member States or on data emanating from within the EU. There will likely be one-off costs for CJS agencies as they have to dedicate resources to ensuring that staff are aware of and comply with the new rules when they carry out domestic data processing.

Regulator

23. There will be a resource implication for the ICO if there is an increase in the scope of the Directive. This is because there will be a greater quantity of data processing that must be regulated and will therefore cost more to continue to work on it at the current level.

FREE SUBJECT ACCESS REQUESTS

Description

24. The proposed Directive says that subjects access requests (SARs), in which data subjects can access personal data held about them, must be provided free of charge in most circumstances. The only exception to this rule of free SARs that is allowed for is if the requests from a data subject are vexatious, repetitive or voluminous. However, it is for the data controller to bear the burden of proof that the requests fall into any one of these categories.
25. The present DPFD contains no restriction on what fees may be charged and under the UK Data Protection Act, a fee of no more than £10 may be charged for SARs to contribute towards administrative costs and to discourage unnecessary or frivolous requests.

Benefits of Free Subject Access Requests

Individuals

26. There will be a benefit for individuals of not having to pay £10 per request. Also, individuals who have been deterred from making requests may be encouraged to do so now, and may benefit from being able to correct their personal data if appropriate and in any case to access it for their own satisfaction.

Costs of Free Subject Access Requests

Courts and Tribunals Service

27. The Directive provides that Member States must provide for the right of to a judicial remedy if rights laid down the Directive have been infringed as a result of the processing of their personal data contrary to its provisions. Courts and Tribunals may in particular see an increase in their costs if there are a greater number of judicial appeals arising from a greater number of SARs which data subjects consider have not been complied with fully.

Other Criminal Justice System Agencies

28. If SARs become free, there will be two main impacts – the loss of the £10 fee and the cost of dealing with more requests. While the proposals allow for CJS data controllers to charge a fee where requests are ‘vexatious’ because of their repetitive character, or the size or volume of the request, the burden will be on the controller to prove the ‘vexatious character’ of the request. Therefore, even those requests that are vexatious will still present a cost to data controllers as they will need to state why they are refusing the request.

29. Many CJS agencies, such as SOCA, however, do not charge a £10 fee due to the administrative costs associated with processing a cheque and due to the relatively low number of SARs that they receive. It is therefore particularly important to consider the impact of the change in fee rules in relation to those competent authorities that receive many requests already.
30. Conversely, UKBA receives 22,000 SARs a year and therefore stands to face increased costs of up to £220,000 a year if it is unable to charge a £10 fee. This may rise even more if the number of SARs they receive also rises. UKBA has previously stated its preference for an *increase* in the fee limit to above the present £10 level. The impact on UKBA can therefore be said to be relatively high. The Association of Chief Police Officers Criminal Records Office receives around 60,000 requests per annum according to their response to the MoJ Call for Evidence on the DPA that ended in October 2010. They will therefore face considerable increased costs also.
31. Evidence received from the MoJ's 2010 Call for Evidence put the cost of compliance with a SAR between £100 and £500, with a particularly high volume of SARs being sent to public sector bodies. It is therefore fair to estimate that the cost to CJS agencies would exceed £3 million.

Regulator

32. If there are more SARs, then it is likely that there will be more cases where all or some of a SAR is refused by the data controller. If this happens, data subjects have the right to request that the ICO examine the case for releasing the data following the SAR. Therefore, there will be an increased cost for the ICO in dealing with such cases as they will be more frequent than at present.
33. Member States are also required to provide for the right to a judicial remedy against decisions of a supervisory authority. If an individual is disappointed by the decision of the ICO following a complaint about the handling of a subject access request by a data controller, the ICO may also need to make statements pursuant to any litigation which the data subject may wish to bring. This also represents a cost. The 2011/12 ICO budget puts aside more than £80,000 per year on legal costs for data protection. An estimate would therefore increase that cost by around £20,000 if there is a 25% increase in the number of cases being referred.

RIGHTS TO ERASURE AND RECTIFICATION

Description

34. Data subjects have an increased right to erasure of data that does not conform with the data processing principles, the rules for lawfulness of processing or the rules for processing of sensitive personal data. The data controller must erase personal data that does not conform to these requirements "without delay" if a data subject requests this of them. Additionally, the obligation is on the controller to verify the legitimacy of the data subject's erasure request and to set out their reasoning if they refuse the request.
35. Data subjects also have the right to rectification, under which incorrect data must be corrected and incomplete data must be completed. The data subject may now exercise this right directly to the data controller and it is the latter's obligation to set out their reasoning if they refuse the request.

36. However, there are exemptions to these rights. For example, under article 16(3) instead of erasure the data controller can mark the personal data (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the personal data have to be maintained for purposes of proof; (c) the data subject opposes their erasure and requests the restriction of their use instead.

Benefits of Rights to Erasure and Rectification

Individuals

37. Individuals will benefit from greater control over their data and rights. They will be able to satisfy themselves that their personal data is being processed according to law and that it can be erased if this requirement is not met. They can also be assured that data held concerning them is accurate and that it can be amended or completed if not.

Costs of Rights to Erasure and Rectification

Police

38. The Police may be particularly impacted by these proposals as data subjects may wish for their personal data to be deleted after a criminal investigation is concluded and the data is no longer immediately required for processing. There are fifty-two territorial police forces across the UK and it is likely that personal data may have been shared across several or even all of these bodies, meaning a particular adverse impact may be had on the police.

Other Criminal Justice System Agencies

39. The requirement to investigate the correctness and lawfulness of personal data held and then to delete or rectify it if necessary, indicates that there may need to be staff dedicated to this purpose, thereby increasing costs for data controllers.
40. There may also be difficulties in ensuring that all copies of the data have been found and that deletion or rectification is ensured in all instances. In particular, the need to know where all copies of data are may require additional costs in terms of keeping of documentation.
41. Demonstrating the legitimacy of not complying with the data subject's request, which is an obligation that falls to data controllers, may not always be easy and straightforward and could thereby represent another cost.

Regulator

42. There will also be enforcement costs for the ICO in ensuring that CJS agencies uphold these rights, given that there may well be a high demand for it, with subsequent costs for the Courts to process cases.

DATA BREACH NOTIFICATIONS

Description

43. If there is a personal data breach, controllers will have an obligation to notify, “without undue delay and, where feasible, not later than 24 hours after having become aware of it, the personal data breach to the supervisory authority”. There is also an obligation to notify the data subject “without undue delay” if it is appropriate to do so.

Benefits of Data Breach Notifications

Criminal Justice System

44. Honest notifications may also help increase confidence in CJS agencies by data subjects, if the latter are reassured that they (or the supervisory authority) will be informed if there is a breach.
45. Speedy reporting of data breaches may help to reduce costs in the form of fines applied to CJS agencies if the negative impacts of the breach can be mitigated by notifying the supervisory authority and possible the data subjects and taking appropriate action.

Individuals

46. Individuals will benefit from knowing that their data is being kept safe and that they will be notified, if appropriate, if there has been a breach. This will avoid situations where harmful breaches have occurred, but data subjects were not informed until some time after the event.

Costs of Data Breach Notification

Criminal Justice System

47. It is likely that this proposal could have a large impact on CJS agencies. The requirement to notify will have a cost in terms of identifying, clarifying and communicating breaches. Furthermore, time-limited breach notifications may inadvertently divert resource and focus away from remedying a breach, resulting in further consequences arising from the initial breach; this will compound the impact upon CJS agencies. However, with the “without undue delay” caveat, some of these impacts may be overcome.
48. Although individuals may, as was outlined above, may have increased confidence in CJS agencies if they know they will receive notification in the case of a data breach, if these notifications are received too often, then it may erode confidence in CJS agencies.
49. It is not likely that large-scale breaches will occur very often, and therefore these costs may not be incurred often. However, a cost will exist in regards to data breaches that cause negligible or no harm, but which nonetheless need to be reported. These notifications will bear a cost and no tangible benefits (indeed a further cost may exist if the notification causes undue alarm or lack of confidence).
50. CJS agencies may also be prosecuted, directly or via the ICO, if they have failed to protect personal data. This will represent a cost to them in terms of defending themselves in Court and in paying any fines and/or compensation that may result from these cases.

Regulator

51. There will be an increase in costs for the supervisory authority, owing to their obligation to receive these notifications, process them and take any necessary actions. The possibility of the Commission to add further requirements in these notifications via delegated acts also acts as a potential cost if used and in any case adds uncertainty.

Individuals

52. Individuals may be adversely impacted if they begin to receive numerous notifications for breaches that have trivial or no impact on their own data security. This may in the first instance cause them to lose peace of mind and create undue alarm. In the long-term, however, data subjects may come to be “desensitised” by these breach notifications and could therefore ignore a notification of a more serious breach that does impact them adversely.

DATA PROTECTION OFFICERS

Descriptions

53. Controllers will be obligated to designate data protection officers (DPOs), all of whom must have “professional qualities” and “expert knowledge of data protection law and practices”. The proposed Directive prescribes a list of eight tasks that the DPO will have to fulfil, including the monitoring of documentation kept by processors and controllers, to monitor the implementation of data protection policies and to consult with the supervisory authority.
54. However, in regards to base case comparisons, it is likely that many CJS agencies, especially larger ones, already have staff employed to serve specific data protection obligations. For example each territorial police force is almost certain to have one. Analysis therefore focusses on the *obligations* for the appointments of DPOs and the *prescription* found within the proposed Directive on the tasks and role of the DPO.

Benefits of Data Protection Officers

Criminal Justice System

55. The compulsory appointment of a DPO will ensure that all areas of data processing within all CJS agencies are aware of the obligations under data protection law and that practices are implemented that conform to these laws. This is likely to help increase compliance and therefore increase the operational efficiency of CJS agencies, as well as helping them to avoid fines and other adverse effects of data breaches, improper practices, etc.

Wider Society

56. Data Protection Officers will help contribute to the fostering of good practice by data controllers and processors as well as helping their adherence to the specific rules as laid down in law. There would therefore be a general benefit to wider society in terms of confidence in data processing by CJS agencies and the avoidance of the negative impacts associated with data breaches and a general lack of care towards the handling of personal data.

57. As part of this, the ICO will also benefit in cost terms if there is a reduction in the number of complaints and other cases that they must deal with that are associated with bad data processing practices if these are mitigated by DPOs.

Costs of Data Protection Officers

Criminal Justice System

58. The tasks are quite broad and therefore larger organisations will undoubtedly be required to appoint more than one DPO in order to fulfil their obligations. The salaries to be paid to these individuals would likely need to be quite high as they are required to have expert knowledge that is unlikely to come cheaply.
59. The prescriptive list of tasks, applicable to each and every DPO, will also represent a cost to CJS agencies as it will mean their DPOs may be completing tasks that are not applicable or appropriate for the given agency. Appointing DPOs with more general obligations to foster good practice and compliance with the rules would help reduce costs via increased effectiveness.
60. Crucially, there is no threshold for the size of an agency regarding the DPO obligation; all controllers are obligated to have one. Whilst the Directive does allow for a single DPO to serve across several entities, there will still undoubtedly be cases where small agencies will nonetheless need to appoint one themselves. An estimate of the annual salary costs for a DPO would be £50,000, which would be a cost borne by each agency that is required to appoint one.

DOCUMENTATION AND RECORDS

Description

61. The Directive contains obligations for controllers to keep documentation relating to each and every piece of data processing that has been carried out.
62. These documents must contain details of: personal details of the controllers and processors, the purposes of the processing, recipients of the data and international transfers. Furthermore, records must be kept of each processing operation carried out on data, sometimes requiring further details about the purpose, date and time of the actions.

Benefits of Documentation and Records

Criminal Justice System

63. The keeping of records and documentation can be considered good practice that will help data controllers and processors to better conform to data protection rules. This will benefit CJS agencies if it allows them to avoid the fines or judicial proceedings associated with violating data protection rules. It will also enable agencies to demonstrate more easily how their practices conform to the law.
64. However, these benefits must be read alongside the base case, which is the level of useful and beneficial documentation that is already kept. It is likely that a large degree of good practice exists already within CJS agencies regarding documentation and records, especially within Courts where proceedings are

necessarily public. Therefore, it is likely that a large part of the benefit derived from documentation and records exists already.

Wider Society

65. The keeping of documentation and records may help contribute to the fostering of good practice by data controllers and processors as well as helping their adherence to the specific rules as laid down in law by ensuring that only legal processing is carried out and noted. There would therefore be a general benefit to wider society in terms of confidence in data processing by CJS agencies and the avoidance of the negative impacts associated with data breaches and a general lack of care towards the handling of personal data.
66. As part of this, the ICO will also benefit in cost terms if there is a reduction in the number of complaints and other cases that they must deal with that are associated with bad data processing practices if these are mitigated by the keeping of good documentation. Additionally, the existence of these documents and records will facilitate ICO investigations to proceed more easily and quickly as the evidence will already exist detailing the data processing other actions.

Costs of Documentation and Records

Criminal Justice System

67. The keeping of documentation and records will require data processors to spend more of their time keeping up to date with this paperwork, which means more resources will be dedicated to this activity. This may therefore represent a cost to CJS agencies if it requires them to hire more staff to cover this loss in productivity.
68. There may also be costs present in creating automatic filing systems to store the documentation as well as the cost of accessing them at the request of the supervisory authority.

PRIOR CONSULTATION

69. The new Directive contains an obligation for CJS agencies to consult with the supervisory authority prior to processing sensitive personal data on a new filing system.

Benefits of Prior Consultation

Criminal Justice System

70. Consultation to establish the safety and legal compliance of new filing systems may benefit CJS agencies if it helps them to prevent data breaches or other violations of data protection rules. Additionally, the advice of the data protection experts at the supervisory authority may help agencies to use filing systems that are the most efficient and effective for their work and therefore reduce costs.

Regulator

71. The ICO will be able to use prior consultation to raise concerns that they may have with new data processing methods. This may be able to help reduce any negative impacts of such systems occurring and such pre-emptive action will save the ICO resources by eliminating the need for them to investigate later on.

Individuals

72. Prior consultation may help to prevent new data processing systems that have the potential to lead to data breaches or other violations of data protection law. This will be a benefit to data subjects who will have a reduced chance of having their data processed in a new system that could violate their data protection rights.

Costs of Prior Consultation

Criminal Justice System

73. The definition of “a new filing system” may be hard to define and therefore agencies may need to overcompensate and consult far too much in order to avoid breaching the rules. This would represent a cost to them if they had to dedicate resources to this consultation rather than more meaningful data processing. Conversely, ambiguities may also mean agencies inadvertently do not consult when deemed necessary and therefore incur penalties.
74. The ICO may, especially in the months following implementation of the Directive, become inundated with consultation requests that could represent a significant resource burden and cost to them.

Regulator

75. The ICO will need to be consulted by data controllers when they have a new filing system for data processing. There will therefore be an increased resource requirement in order to hear these consultations and possibly to respond and/or take further action.

RULES FOR INTERNATIONAL TRANSFERS

76. The proposed Directive contains new rules regarding whether or not personal data may be transferred by CJS agencies outside of the European Economic Area (EEA).
77. Rules require an adequacy decision from the Commission for the third country in question for a transfer to be permitted. Previously, the ICO was able to make these adequacy decisions, although it did so rarely. If an adequacy decision does not exist, the Directive requires there to be “appropriate safeguards” or other requirements to be fulfilled regarding the necessity and value of the transfer. This provision is likely to cover most transfers, except bulk or regular ones.

Benefits of Rules for International Transfers

Regulator

78. There will be a very small benefit to the ICO in no longer having to make adequacy decisions as this is now fully within the remit of the European Commission

Individuals

79. Individuals benefit from rules regarding international transfers as they can be more assured that their personal data will not be transferred outside of the EEA to a state which does not have adequate data protection rules. However, it is not known whether the new regime will mean that transfers become safer.

Costs of Rules for International Transfers

Criminal Justice Agencies

80. The new requirements for Commission adequacy decisions is likely to lead to an increased difficulty in CJS agencies being able to transfer data out of the EEA as the Commission has set down additional rules regarding its granting of adequacy decisions. This may mean that CJS agencies are less able to share data internationally, a concern that has been raised by the United States in a recent non-paper.
81. There is a chance that, if EU Member States find it harder to share data internationally, then non-EEA states may be reluctant to send data to Member States, thereby hindering the law enforcement capabilities of these agencies.

Wider Society

82. As was outlined above, non-EEA states may become more reluctant to send personal data necessary for crime prevention to EU Member States if the new rules mean that there is less reciprocal transfer of such data from within the Union. Wider Society may therefore lose out if there is an increased risk from criminal acts being performed if there is less international data sharing.

4. SUMMARY OF IMPACTS

Table 1 Benefits and Costs of Proposals				
		Criminal Justice System	Regulator	Individuals
Internal Processing	Benefits	<ul style="list-style-type: none"> Ease of international sharing due to assurances of adequacy 	-	<ul style="list-style-type: none"> Guarantees of data protection for data processed internally
	Costs	<ul style="list-style-type: none"> More data processing to be regulated 	<ul style="list-style-type: none"> More data processing to be regulated 	-
Free Subject Access Requests	Benefits	-	-	<ul style="list-style-type: none"> Reduction in cost to access, greater ease and speed of access
	Costs	<ul style="list-style-type: none"> No fee to help pay for costs of SARs Increased number of SARs Obligation to demonstrate why SARs are rejected/charged for 	<ul style="list-style-type: none"> Increased number of SARs cases to adjudicate 	-
Rights to Erasure and Rectification	Benefits	<ul style="list-style-type: none"> Less processing to do on incorrect/unlawful data 	-	<ul style="list-style-type: none"> Greater control over and access to their own data
	Costs	<ul style="list-style-type: none"> Additional costs of dedicating staff to this task Difficulty in tracking all deletion and rectification 	<ul style="list-style-type: none"> Increased number of erasure or rectification cases to adjudicate 	
Data Breach Notifications	Benefits	<ul style="list-style-type: none"> Increased confidence in CJS agencies Mitigation of harmful effects of breach if acted upon swiftly 	-	<ul style="list-style-type: none"> Increased confidence in their personal data being kept safe Increased transparency if there is a breach
	Costs	<ul style="list-style-type: none"> Necessity of devoting time and staff to notifications Waste of resources if breach is of trivial harm 	<ul style="list-style-type: none"> Cost of receiving and acting upon notifications 	-
Data Protection Officers	Benefits	<ul style="list-style-type: none"> DPOs help to foster good practices 	<ul style="list-style-type: none"> DPOs help to foster good practices, reducing the need for ICO intervention 	<ul style="list-style-type: none"> DPOs help to foster good practice, ensuring data subjects' rights are better protected
	Costs	<ul style="list-style-type: none"> Cost of appointing experts to be DPOs 	-	-

		<ul style="list-style-type: none"> • Too many tasks for DPOs may divert resources • No threshold: particular impact on smaller agencies 		
Documentation and Records	Benefits	<ul style="list-style-type: none"> • Keeping of records helps to foster good practices 	<ul style="list-style-type: none"> • Keeping of records helps to foster good practices, reducing the need for ICO intervention • Keeping of records enables ICO to more quickly establish facts when intervening 	<ul style="list-style-type: none"> • Keeping of records helps to foster good practice, ensuring data subjects' rights are better protected
	Costs	<ul style="list-style-type: none"> • Cost of employing staff to keep records and documentation • Cost of filing systems to store records and documentation 	-	-
Prior Consultation	Benefits	<ul style="list-style-type: none"> • Potential risks associated with a new system may be averted 	<ul style="list-style-type: none"> • Potential risks associated with a new system may be averted, reducing the need for ICO intervention 	<ul style="list-style-type: none"> • Potential risks associated with a new system may be averted, ensuring data subjects' rights are better protected
	Costs	<ul style="list-style-type: none"> • Cost of devoting resources to consultation • Ambiguity of terms may mean unnecessary consultation occurs 	<ul style="list-style-type: none"> • Cost of devoting staff to dealing with consultation and taking necessary actions in response 	-
New Rules for International Transfers	Benefits	-	<ul style="list-style-type: none"> • ICO will no longer need to assess adequacy of non-EEA countries 	<ul style="list-style-type: none"> • Greater assurances that personal data will not be transferred to inadequate non-EEA countries
		<ul style="list-style-type: none"> • Reduced capacity to send and receive data internationally 	-	<ul style="list-style-type: none"> • Concern of increased criminality if international criminal data sharing is hindered