

Implications of the European Commission's proposal for a general data protection regulation for business

Final report to the Information Commissioner's Office

Prepared by



May 2013

About London Economics

London Economics is one of Europe's leading specialist economics and policy consultancies. Based in London and with offices and associate offices in five European capitals, we advise an international client base throughout Europe and beyond on economic and financial analysis, litigation support, policy development and evaluation, business strategy, and regulatory and competition policy.

Our consultants are highly-qualified economists who apply a wide range of analytical tools to tackle complex problems across the business and policy spheres.

Our approach combines the use of economic theory and sophisticated quantitative methods, including the latest insights from behavioural economics, with practical know-how ranging from commonly used market research tools to advanced experimental methods at the frontier of applied social science.

We are committed to providing customer service to world-class standards and take pride in our clients' success. For more information, please visit www.londecon.co.uk.

Head Office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.

w: www.londecon.co.uk e: info@londecon.co.uk

t: +44 (0)20 7866 8185 f: +44 (0)20 7866 8186

Wherever possible London Economics uses paper sourced from sustainably managed forests using production processes that meet the EU eco-label requirements.

Copyright © 2013 London Economics. Except for the quotation of short passages for the purposes of criticism or review, no part of this document may be reproduced without permission.

Contents

Page

Glossary	v
Executive summary	vi
1 Background & context	12
1.1 The ICO's brief	12
1.2 The European Commission's proposal for a general data protection Regulation	13
2 Provisions of the proposed Regulation	14
3 Impact on business	17
3.1 Overall expected costs and benefits	19
3.2 Costs and benefits of key provisions	21
3.3 Second-order effects	50
4 Priorities for the ICO	52
4.1 Evidence on businesses' relationship with the ICO	53
4.2 Practical support and guidance the ICO could provide to businesses	54
4.3 Summary	58
References	62
Annex 1 Survey of businesses	65



Tables, Figures & boxes

Page

Table 1: Estimated costs of provisions on consent by business activity	29
Table 2: Costs and benefits of provisions strengthening data subject rights for business	33
Table 3: Costs and benefits of provisions on breach notifications, administrative sanctions and DPIA/DPO requirements	40
Table 4: Summary of studies on market reaction to security breaches	49
Table 5: Likelihood of approaching the ICO in the future	54
Table 6: Sectoral distribution of survey participants	78
Table 7: Size of firms that employ staff with data protection responsibilities	78
Table 8: Data intensity of firms that employ staff with data protection responsibilities: number of customer records	79
Table 9: Data intensity of firms that employ staff with data protection responsibilities: number of third party records	79
Table 10: Risk of harm to business from data security concerns by firms that employ staff with data protection responsibilities	80
Table 11: Expected additional cost of provision on DPOs by firms that employ staff with data protection responsibilities	80
Table 12: Restrictions on the development of new business activities or processes	80
Table 13: Data intensity of firms that had previous contact with the ICO: number of customer records	81
Table 14: Data intensity of firms that had previous contact with the ICO: number of third party records	82
Table 15: Frequency of ranking score for policy tools available to the ICO	83
Table 16: Regression output: expected additional cost of new Regulation	87
Table 17: Regression output: expected additional cost of new Regulation	88
Table 18: Regression output: expected additional cost of provision (1 = no additional costs; 5 = substantial additional costs)	95
Figure 1: Current yearly spending and expected additional one-off costs, by number of customer records held	20
Figure 2: Current yearly spending and expected additional ongoing costs, by number of customer records held	21
Figure 3: Summary of costs	22
Figure 4: Summary of benefits	23
Figure 5: Number of correct answers on knowledge of provisions	24
Figure 6: Uncertainty about the proposed measures (% don't know vs % wrong)	25
Figure 7: Distribution of respondents' answers to the question on the definition of personal data (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	27
Figure 8: Distribution of respondents' answers to the question on consent requirements (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	30
Figure 9: Distribution of respondents' answers to the question on data minimisation (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	32
Figure 10: Distribution of respondents' answers to the question on subject access requests (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	35

Tables, Figures & Boxes

Page

Figure 11: Distribution of respondents' answers to the question on the right to be forgotten (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	37
Figure 12: Distribution of respondents' answers to the question on data portability (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	38
Figure 13: Distribution of respondents' answers to the question on breach notification (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	42
Figure 14: Distribution of respondents' answers to the question on DPIAs (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	42
Figure 15: Likelihood of employing staff with data protection responsibilities given firm size	43
Figure 16: Likelihood of employing staff with data protection responsibilities given number of customer records held	44
Figure 17: Likelihood of employing staff with data protection responsibilities given risk of harm to business from data security concerns	44
Figure 18: Proportion of firms that employ staff with data protection responsibilities and expectations of costs from DPO provision	45
Figure 19: Distribution of respondents' answers to the question on DPOs (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	46
Figure 20: Distribution of respondents' answers to the question on administrative sanctions (<i>left</i>); and distribution of related cost expectations (<i>right</i>)	47
Figure 21: Benefit of holding customer data by firms that regularly transfer personal data crossborder	51
Figure 22: Likelihood of having prior contact with the ICO given the number of customer records	54
Figure 23: Average ranking per support option	55
Figure 24: Distribution of rankings for each support option	55
Figure 25: Average ranking of support options by firm size	56
Figure 26: Knowledge gaps and business risk by sector	58
Figure 27: Likelihood of employing staff with data protection responsibilities given number of third party records	79
Figure 28: Knowledge of provisions by volume of data (on customers and third parties) held by companies	81
Figure 29: Likelihood of having prior contact with the ICO given the number of third party records	82
Figure 30: Average ranking of support options by knowledge of provisions	83
Figure 31: Average ranking of support options by previous contact with the ICO	84
Figure 32: Average ranking of support options by sector	85
Figure 33: Average ranking of support options by data intensity (no. of records held)	86
Figure 34: Predictors of overall expected additional cost	89
Figure 35: Predictors of overall expected additional cost of Regulation, accounting for regular cross-border transfer of data	89
Figure 36: Predictors of additional cost related to the definition of personal data	90
Figure 37: Predictors of additional cost related to consent requirements	90
Figure 38: Predictors of additional cost related to data minimisation	91
Figure 39: Predictors of additional cost related to the subject access requests	91
Figure 40: Predictors of additional cost related to the right to be forgotten	92

Tables, Figures & boxes

Page

Figure 41: Predictors of additional cost related to data portability	92
Figure 42: Predictors of additional cost related to breach notification	93
Figure 43: Predictors of additional cost related to data protection impact assessments	93
Figure 44: Predictors of additional cost related to data protection officers	94
Figure 45: Predictors of additional cost related to administrative sanctions	94

Glossary

Terminology abbreviations

CBI	Confederation of British Industry
DMA	Direct Marketing Association
DPA	Data Protection Act 1998
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EEA	European Economic Area
FSB	Federation of Small Businesses
IAB	Internet Advertising Bureau
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IP	Internet Protocol
MoJ	Ministry of Justice
RTBF	Right to be forgotten
SAR	Subject Access Request
SME	Small or Medium-sized Enterprise

Executive summary

Box 1: Key findings

- A lack of understanding about the provisions in the EC's proposed general data protection Regulation persists across business. Uncertainty is pervasive across the provisions of the proposed regulation, and affects more abstract and unsettled aspects, such as the obligations of data controllers under the so-called right to be forgotten, as well as seemingly straightforward changes such as those regarding administrative fines and the appointment of Data Protection Officers.
- The majority of businesses are unable to quantify their current spending in relation to data protection responsibilities under existing law – and this persists in relation to estimates for expected future spending under the new proposals. This uncertainty indicates that existing evidence on the financial impact of the regulation is difficult to corroborate. Further research is required to clarify some important issues, such as the role of privacy and data protection in determining the level and intensity of consumer participation in online markets.
- The lack of understanding that the research reveals strongly indicates that there is a key role for the ICO to play in educating and supporting businesses to increase their awareness and understanding of the forthcoming changes. The ICO's priorities for supporting business in implementing the new Regulation should focus on providing guidance on the areas of the new provisions which are shown to be misunderstood – for example the 'right to be forgotten', but also the new rules on fines, the appointment of Data Protection Officers, Subject Access Requests and data portability.
- While uncertainty affects all industries, the ICO should focus its liaison work on organisations involved in data-intensive activities, who face economic risks from breaches of data protection rules – which map onto the risks for data subjects; and organisations who are active in sectors where knowledge of the rules seems to be particularly low. The study finds evidence that the service sector in general, and specifically health, finance and insurance and public administration¹ should be prioritised.

Objectives of the study

On 25 January 2012, the Directorate General for Justice at the European Commission announced its legislative proposal for the protection of individuals with regard to the processing and use of personal data.

The Information Commissioner's Office (ICO) appointed London Economics to undertake a study to objectively evaluate the potential implications of the draft proposals for a new EU data protection legislative framework for business. Within this context, three areas are of special interest to the ICO:

¹ Our survey (reproduced in Annex A1.2, p. 66) was directed at staff with data protection responsibilities in UK businesses. No additional screening for private sector employment was undertaken, which resulted in a number of respondents whose profile information indicates 'public sector' status. In the sector "public administration and defence" this includes of 85% respondents. However, some ambiguity remains, as the classification "public administration" is not restricted to government bodies: private units performing typical 'public administration activities' are also classified here (Office of National Statistics, UK Standard Industrial Classification of Economic Activities 2007, Structure and explanatory notes).

- 1) The overall net objective cost to UK business to comply with the relevant provisions in the proposed new data protection regulation, including one-off and recurring costs.
- 2) The articles in the proposed regulation that will cause the greatest challenges – and/or benefits – for business in terms of compliance.
- 3) The types of practical support and guidance the ICO could provide to businesses in the implementation of the proposed measures.

London Economics' approach

The study is not intended as a comprehensive analysis of the costs and benefits of the proposed regulation and its application in practice. The purpose of the study is to provide independent and objective research to further the ICO's understanding of the potential implications of the Commission's new data protection proposals for business.

Objective evidence will enable the ICO to better assess some of the more questionable costs estimates for implementation of the new proposals that have been put forward by business and others. London Economics evidence comes from two sources:

- **Primary evidence:** a unique survey of 506 individuals with data protection responsibilities in their place of work, taken at random from the UK business population. The survey was conducted in February 2013.
- **Secondary evidence:** the study draws on the ICO's initial response to the draft proposals and a background paper that has been published alongside the specifications of the study exploring the practical implications of specific provisions in the proposed regulation for business. Other important sources are the responses to the Ministry of Justice's call for evidence and the European Commission's own impact assessment of the proposals.

The study adds to the evidence base by shedding light on the level of uncertainty that exists within the UK business population regarding the scope of the Regulation and its cost impact. Furthermore, the study investigates the influence of business characteristics on cost expectations.

Overall costs

Uncertainty

Uncertainty persists about the scope of some provisions of the proposed Regulation and the interpretation that will guide the enforcement of the new rules. Different estimates of the impact vary widely, underlining the uncertainty surrounding the effects of the proposed Regulation:

- The European Commission estimated that the new legislative framework would bring net savings for economic operators of €2.3 billion.
- The Ministry of Justice estimated a net cost to UK business of between £80 million and £320 million per year.

A large majority of respondents to the London Economics survey are unable to quantify current spending on data protection (82%). When asked about expectations of future spending (once the new Regulation comes into force) an even larger proportion of respondents (87%) are unable to

provide any estimates (both for one-off adjustment costs and additional yearly compliance costs). Of the remaining 13%, 8% expect zero additional costs.

Two further results emerge:

- Current and expected additional spending on data protection increases substantially for firms holding more than 100,000 records of personal data.
- Average costs (current and expected) are driven by a small number of large observations.

This suggests that the evidence put forward by stakeholders needs to be judged in relation to the fact that firms who a) are able to put a figure on their data protection expenditure and b) possess large volumes of personal data, are not representative of the UK business population as a whole.

On the specific issue of the proposal to appoint a Data Protection Officer (DPO), the London Economics survey reveals three important facts:

- the vast majority of companies with over 250 employees already employ staff with a job role focused on data protection compliance;
- the vast majority of companies who keep more than 100,000 records already employ staff with a job role focused on data protection compliance; and
- companies that perceive greater risk for their business from breaches of data security or concerns about data security are more likely to have employees with a job role focused on data protection compliance.

These facts suggest that the majority of firms to which this provision applies are already satisfying the requirement and need not expend significant additional resources to comply.

Implications for the overall cost assessment

Average costs (current and expected) are driven by a small number of large observations. The skewness of expected costs means that average figures on expected costs are not informative about the incidence and the distributional aspects of the costs and benefits to be expected from the proposals.

Firms who derive large benefits from holding personal data and firms who perceive they risk considerable damage from breaches of security or concerns over data security expect higher costs. This suggests that the ICO should focus its support efforts on these firms. Consultations have shown that certain types of data-intensive businesses, for example in the financial services, online services and marketing sectors, face specific challenges in this regard and thus deserve special attention. Survey evidence assembled in this study also confirms that perceived risk increases with company size (measured by number of employees) and the number of records of personal data a company holds (the two are also positively correlated).

At the same time, it should be recognised that firms who are able to put a figure on their data protection expenditure, and who possess large volumes of personal data, are not representative of the UK business population as a whole.

For a number of provisions, companies that do not have accurate knowledge of the proposed Regulation report systematically higher additional costs relative to the base (status quo). This

provides support for the claim that poorer knowledge of the new provisions is associated with higher-than-average cost expectations.

Existing estimates of the costs of the proposed measures that do not take knowledge of the provisions – and the inherent uncertainty associated with some of the provisions – into account are likely to be misleading. Increasing awareness about the forthcoming changes to data protection obligations among firms, especially firms facing high risk from data breaches and firms with low level of knowledge of the planned provisions is as important a task for the ICO as ensuring clarity of the measures to be enacted. Our survey confirms that organisations in the service sector in general, and specifically in health and social work, financial and insurance services and public administration² warrant special attention by the ICO.

Compliance challenges

Stakeholders have identified a number of provisions of the new Regulation as potentially burdensome to business. Concerns arise from two sources:

- 1) expectations of direct costs (or the risk thereof); and
- 2) uncertainty about the scope of the provisions and the extent to which they will affect established business practices or close off new and emerging business areas.

In the first category, the following provisions give rise to concrete expectations of additional costs:

- subject access requests (Articles 12);
- breach notification within 24 hours (Article 31);
- data protection impact assessments prior to risky processing operations (Article 33);
- obligation to appoint a data protection officer (Articles 35-37); and,
- imposition of large fines for failure to comply (Article 79).

Provisions in the second category, where the cost impacts are more indirect, are:

- the ‘right to be forgotten’(Article 17);
- data portability (Article 18);
- lack of clarity around some definitions (Article 4);
- higher standard of consent (Articles 4(8) and 7); and
- data minimisation (Article 5).

The reported views on the challenges arising from the changes to be introduced by the new Regulation have to be seen in the context of low levels of knowledge about the actual content of the provisions. As many as 40% of companies that participated in our survey have inaccurate knowledge of all 10 provisions considered. None of the survey respondents accurately describe all 10 provisions. This suggests that a large proportion of companies in the UK do not have a clear grasp of how data protection regulation will change once the EC proposals are enforced. This lack

² See footnote 1 above.

of understanding persists for companies that hold over 100,000 records of personal data. Companies in the services sector are most likely to record high levels of uncertainty.

However, this lack of understanding is not necessarily the result of ignorance on the part of firms, but may also be driven by the complexity of the proposed Regulation and the persistent uncertainty about the meaning and implications of some of its provisions.

There is some indication that low levels of knowledge – in particular with regards to the rules on fines and data minimisation – contribute to higher cost expectations. This suggests that efforts by the ICO to improve data controllers' knowledge of the proposed Regulation could lead to more realistic and in many cases lower cost expectations.

Priorities for the ICO

Evidence collected from stakeholders suggests that certain types of data-intensive businesses (such as those active in digital marketing and financial services) expect significant cost increases as a result of the proposed Regulation. Moreover, impact assessments have found that the overall costs to business of implementing the proposals will be substantial, even if they lead to a net benefit for the economy as a whole. The ICO should ensure that the implementation strategy takes into account the concerns raised by the business community and minimises the implementation cost, while at the same time achieving the EC's objectives in terms of data protection, legal harmonisation and consumer privacy.

Our research identifies some of the parameters that define a successful strategy to support the implementation of the new Regulation for the benefit of UK business and data subjects. The London Economics survey shows that:

- 21% of firms in the sample have been in contact with the ICO on a previous occasion.
- Companies that handle fewer records of personal data are more likely to have had contact with the ICO in the past.
- Companies who had previous contacts with the ICO are much more likely to approach the ICO concerning the new Regulation.

As part of its wider engagement with business, the ICO should consider the evidence that the report provides about where engagement could be reviewed and potentially expanded, and the possibility of this having a lasting effect.

The survey provides clear insights into the types of support from the ICO businesses would see as beneficial:

- Provision of clear and concise guidance about the scope of the new provisions (changes from the status quo) available on the ICO's website is unambiguously the form of ICO support that is seen as most beneficial.
- Second to this is a contact point (telephone helpline, email, live chat, etc) to deal with specific questions regarding the new data protection rules.
- ICO-approved accreditation or certification schemes on specific areas of compliance are seen as the least beneficial.

These findings indicate the following priorities for the ICO in fulfilling its regulatory responsibility to help organisations understand their new responsibilities whilst continuing to uphold individuals' privacy rights:

- The ICO's approach should focus on making information available and accessible through various channels (both on the website and through its helpline).
- The ICO should focus on raising businesses' awareness of the future ICO guidance and advice that will be available (both on the website and through its helpline). This could take the form of an active information campaign used in parallel with and in support of measures to provide information on demand.
- The ICO should focus on the provision of clear and concise guidance on those provisions that are seen as the most burdensome by business, alongside its activities to alleviate data protection risks for individuals. Survey evidence suggests that even seemingly straightforward measures like the provisions on fines and DPO requirements are insufficiently understood by many businesses. Consequently, all of the measures identified as burdensome in this study merit equal attention by the ICO.

1 Background & context

Box 2: Section summary

- The purpose of the study is to provide the ICO with independent and objective evidence in three areas:
 - the net objective cost to UK business of complying with the proposed data protection Regulation;
 - the provisions that are seen as the most challenging for business; and
 - the areas in which the ICO should focus its support/education efforts.
- Existing evidence reveals considerable uncertainty regarding the impact of the proposed European data protection Regulation on business.

1.1 The ICO's brief

The Information Commissioner's Office (ICO)³ appointed London Economics to undertake a study that objectively evaluates the potential implications of the draft proposals for a new EU data protection legislative framework for business. Within this context, three areas are of special interest to the ICO:

- 1) The overall net⁴ objective cost to UK business to comply with the relevant provisions in the proposed new data protection regulation, including one-off and recurring costs.
- 2) The articles in the proposed regulation that will cause the greatest challenges – and/or benefits –for business in terms of compliance.
- 3) The types of practical support and guidance the ICO could provide to businesses in the implementation of the proposed measures.

The study is not intended as a comprehensive analysis of the costs and benefits of the proposed regulation and its application in practice. Rather, the purpose of the study is to provide independent and objective research to further the ICO's understanding of the potential implications of the Commission's new data protection proposals for business. Objective evidence will enable the ICO to better assess some of the more questionable costs estimates for implementation of the new proposals that have been put forward by business and others.

Furthermore, the research is aimed at strengthening the ICO's efforts to assist business with the implementation of and ongoing compliance with the new Regulation in order to achieve maximum benefits at the least cost to business, while ensuring individuals' privacy rights are upheld.

The study draws on the ICO's initial response to the draft proposals and a background paper that was published alongside the specifications of the study exploring the practical implications of

³ The ICO (<http://www.ico.org.uk/>) is the UK's independent public body set up to promote access to official information and to protect personal information. The ICO regulates and enforces the Data Protection Act, the Freedom of Information Act, the Privacy and Electronic Communications Regulations and the Environmental Information Regulations.

⁴That is, beyond the existing obligations of the current data protection directive (Directive 95/46/EC), other current statutory obligations or standard business practices.

specific provisions in the proposed regulation for business. Other important sources are the responses to the Ministry of Justice's call for evidence and the European Commission's own impact assessment of the proposals.

1.2 The European Commission's proposal for a general data protection Regulation

1.2.1 State of play

On 25 January 2012, the Directorate General for Justice at the European Commission announced its legislative proposals for the protection of individuals with regard to the processing and use of personal data. The proposed framework consists of two EU documents: a draft Regulation legislating for general data protection that is "binding in its entirety and directly applicable in all Member States"⁵; and, a draft Directive (binding as to the result to be achieved but leaving discretion in the choice of form and method to national authorities) with the aim of protecting personal data processed for the purpose of prevention, detection, investigation or prosecution of criminal offences⁶.

The Regulation is expected to come into force in 2015, replacing the 1995 Data Protection Directive (95/46/EC), which is implemented into UK law by the current Data Protection Act 1998 (DPA). The Directive would repeal and replace the existing Data Protection Framework Decision, which was negotiated in 2008, and implemented in the UK through the issuing of an administrative circular.

1.2.2 Uncertain impact

Alongside the publication of the proposals, the European Commission published an Impact Assessment of the overall costs and benefits the proposals would have in the EU. The Commission estimated that the new legislative framework would bring net savings for economic operators of €2.3 billion, from the elimination of legal fragmentation and the ensuing reduction in administrative burdens⁷.

Others, including business organisations such as the Confederation of British Industry (CBI) have expressed the view that the European Commission overestimates the net benefits to business from reduced administrative burdens and fails to accurately quantify the cost of implementing processes and procedures that will be necessary to meet the new obligations. Concern has been expressed that the new Regulation could put European businesses at a competitive disadvantage.

The Information Commissioner's initial analysis of the proposed Regulation suggested that there is a risk that the "implementation of rules perceived as onerous or disproportionate may lead to

⁵ EC COM (2012) 11 final, Article 91

⁶ EC COM (2012) 10 final

⁷ EC SEC (2012) 10 final

more variable standards of compliance by reluctant data controllers.”⁸ This could actually hinder harmonisation within the EU and fail to enhance protection of individuals.

The aim of this study is to assess the impact of the Commission’s proposals on UK businesses. In the next chapters, we:

- summarise the provisions of the proposed Regulation;
- assess the nature and magnitude of such implications based on existing evidence;
- analyse the relationship between businesses’ cost expectations and their knowledge of the provisions and the data-intensity of their business; and
- make recommendations on the type of support that the ICO could provide to businesses to help with the implementation of the Regulation.

The evaluation takes place against a background of persistent uncertainty about the scope of some provisions of the proposed Regulation and the interpretation that will guide the enforcement of the new rules. Uncertainty is pervasive across the provisions of the proposed regulation, and affects more abstract and unsettled aspects, such as the obligations of data controllers under the so-called *right to be forgotten*, as well as seemingly straightforward changes such as those regarding administrative fines and the appointment of Data Protection Officers.

2 Provisions of the proposed Regulation

Box 3: Section summary

- The research focused on the most relevant changes for business - it does not consider all the provisions in the draft Regulation. This section analyses the following specific areas of the Regulation that are likely to have the greatest implications for business:
 - definitions;
 - consent requirement;
 - protection for children;
 - rights of data subjects;
 - obligations on data controllers and processors;
 - data protection officers;
 - international transfer of personal data;
 - cooperation and consistency of supervisory authorities;
 - administrative sanctions.

The draft Regulation specifies:

- principles relating to personal data processing;
- rights of data subjects to access their personal data, have it rectified or erased, object to its processing and not be subject to profiling;

⁸ ICO (2012), p.3

- obligations of data controllers and data processors to provide information to individuals, report breaches of data security and put in place technical and organisational measures;
- rules on transfer of personal data to countries outside the European Economic Area (EEA) and to international organisations;
- rules relating to national “independent supervisory authorities” and how they should cooperate with each other and the European Commission; and
- remedies available to data subjects and administrative sanctions available to supervisory authorities.

The main changes from current data protection law that the proposed Regulation introduces are summarised below.

New and updated definitions

Under Article 4, definitions of key terms such as data subject, data controller and personal data are augmented to account for possible “online identifiers” (e.g. IP addresses, cookie identifiers, etc.), in addition to the “traditional identifiers”. Moreover, the draft proposal introduces new terms such as “location data,” “genetic data” and “biometric data”⁹.

A higher standard for obtaining consent

The 1995 Directive required consent to be given “unambiguously”¹⁰. In the new definition of “data subject’s consent,” the criterion “explicit”¹¹ is added and consent is to be given “in the context of a written declaration”¹². This is intended to eliminate any confusion as to whether consent has or has not been given, and whether it can be implied by a particular action (or inaction).

Greater levels of protection for children

Article 8 of the draft proposal sets out further conditions for the lawfulness of the processing of personal data of children below the age of 13, in relation to consent for online services offered directly to them.

New and strengthened rights for data subjects

The 1995 Directive established the right to access personal data “without constraint at reasonable intervals and without excessive delay or expense”¹³. The new proposed Regulation expands the set of information that must be provided to individuals¹⁴ and removes the ability to charge a fee for subject access requests (SARs)¹⁵.

⁹ EC COM (2012) 11 final, Article 4

¹⁰ Directive 95/46/EC Article 7(a)

¹¹ EC COM (2012) 11 final, Article 4(8)

¹² EC COM (2012) 11 final, Article 7(2)

¹³ Directive 95/46/EC Article 12(a)

¹⁴ EC COM (2012) 11 final, Article 14 and Article 15

¹⁵ EC COM (2012) 11 final, Article 12

It further elaborates and specifies the right of erasure provided for in Article 12(b) of the 1995 Directive and provides the conditions for the *right to be forgotten* (Article 17). This includes the obligation of a controller, who has made the personal data public, to inform third parties on the data subject's request to erase any links to or copies of that personal data.

Article 18 of the proposed Regulation introduces the data subject's right to data portability, i.e. the right to transfer one's personal data from one organisation to another through a "commonly used" electronic format. As a precondition, it provides the right to obtain such data from the controller both in a structured format or raw data form.

New obligations on data controllers and processors

Under current law, data controllers are required to notify the supervisory authority (the ICO in the case of the UK) of their data processing activities and pay a notification fee to the authority¹⁶. The proposed Regulation removes this general notification requirement (and fee) but introduces the obligation for data controllers and processors to maintain documentation of all the processing operations under their responsibility (Article 28)¹⁷.

Data controllers, or processors on their behalf, are required to carry out a data protection impact assessment (DPIA) prior to processing operations that "present specific risks to the rights and freedoms of data subjects" (Article 33). This includes profiling, processing of sensitive types of personal data, monitoring of publicly accessible areas and the use of large-scale filing systems with children's data, genetic data or biometric data.

The Commission proposes a general obligation on data controllers not only to comply with but to *demonstrate* compliance with the data protection legislation (Article 22). Proof of compliance comes in various forms, including maintaining documentation of processing activities and of data protection impact assessments.

Article 30 obliges the controller to implement appropriate technical and organisational measures for the security of processing, as in the 1995 Directive¹⁸. However, it extends this obligation also to processors, irrespective of the contract with the controller.

Article 31 of the proposed Regulation requires that all personal data breaches must be reported to the supervisory authority without undue delay, and where feasible within 24 hours. Currently there is no general obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, although such a requirement has been introduced for Communication Service Providers under the revised e-Privacy Directive¹⁹. Moreover, under the proposed Regulation, "the notification shall be accompanied by a reasoned justification in cases where it is not made within 24 hours".

¹⁶ Directive 95/46/EC Articles 18(1) and 19

¹⁷ Article 28 excludes companies that employ fewer than 250 people and process personal data only as an ancillary activity.

¹⁸ Directive 95/46/EC Article 17(1)

¹⁹ Directive 2002/58/EC Article 4(2)

Mandatory appointment of a data protection officer (DPO)

Both public organisations and private companies (of over 250 employees or whose core activities involve systematic monitoring of data subjects) are required to appoint an in-house data protection officer (Article 35). This builds on Article 18(2) of the 1995 Directive, which provided the possibility for Member States to introduce such a requirement as an alternative to the general notification requirement.

Updated rules on the international transfer of personal data

The proposed Regulation sets out new rules on the transfer of data outside the EEA or to international organisations, requiring in some instances prior approval from the supervisory authority (Article 42).

Mandatory cooperation and enhanced consistency across supervisory authorities

The 1995 Directive loosely states that “supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties²⁰.” The draft Regulation, on the other hand, introduces explicit rules on mandatory mutual assistance, including the obligation to reply to a request of another supervisory authority within a month and prescribed consequences for non-compliance (Article 55).

A new independent supervisory body, the European Data Protection Board (EDPB), is to replace the current Article 29 Working Party (WP29). Under the proposed Regulation, a supervisory authority is required to inform the EDPB whenever it takes any action against a company that operates in multiple Member States (Article 58).

Punitive administrative sanctions in the event of non-compliance

Under current law, the ICO can issue a maximum penalty of up to £500,000 for the most serious breaches of the DPA; moreover the ICO can decide to apply fines or not at its own discretion based on the severity of the consequences of such breaches. The draft proposal introduces a requirement for supervisory authorities to impose prescribed fines of up to €1 million (£0.9 million) or 2% of a firm’s annual global turnover in the event of a violation of the Regulation (Article 79), regardless of the harm caused.

3 Impact on business

Box 4: Section summary

- To obtain new insights into the relationship between businesses’ data-intensity, knowledge of current and proposed data protection rules and cost expectations, London Economics conducted a survey of 506 data protection professionals working in UK companies.
- Findings on cost estimates:
 - A large majority (>80%) of respondents are unable to quantify either current or

²⁰ Directive 95/46/EC Article 28(6) sub-paragraph 2

expected future spending on data protection.

- Current and expected additional spending on data protection increases substantially for firms holding more than 100,000 records of personal data.
- Average costs (current and expected) are driven by a small number of large observations.
- Firms who a) derive large benefits from holding personal and firms b) risk considerable damage from breaches of security or concerns over data security expect higher costs.
- Firms who a) are able to put a figure on their data protection expenditure and b) possess large volumes of personal data, are not representative of the UK business population as a whole.

■ Findings on knowledge of the proposed Regulation:

- 40% of respondents have inaccurate knowledge of all 10 provisions considered; none accurately describe all 10 provisions; the lack of understanding persists for companies that hold over 100,000 records of personal data.
- The lack of understanding is not necessarily the result of ignorance on the part of respondents, but may be a consequence of the complexity of the proposed Regulation and the persistent uncertainty about the meaning and implications of some of the provisions.
- There is some support for the claim that poorer knowledge of the new provisions is associated with higher-than-average cost expectations.

■ Findings on staff in data protection compliance roles:

- The vast majority of companies with over 250 employees already employ staff with a job role focused on data protection compliance;
- The vast majority of companies who keep more than 100,000 records already employ staff with a job role focused on data protection compliance.
- Companies that perceive greater risk for their business from breaches of data security or concerns about data security are more likely to have employees with a job role focused on data protection compliance.

In this section, we gather and review the existing evidence on the implications of the proposed Regulation, drawing on stakeholder consultations, preliminary impact assessments, commentaries and briefs. We thereby identify the provisions in the proposed Regulation that have proven most controversial and are likely to cause the greatest challenges for business in terms of implementation and compliance. Where available, we present evidence that attempts to quantify the additional cost to business of these provisions, differentiating between one-off transitional costs and ongoing compliance costs. At the same time, we draw attention to any articles that might benefit business, and report estimates of these benefits where possible.

In light of the wide range of cost figures that stakeholders have put forward thus far, we integrate the existing evidence with new information gathered through a survey of 506 UK businesses. The dataset is to our knowledge unique in using only data from respondents whose job function includes data protection.²¹ The survey data is used both to gauge the level of understanding of the

²¹ For details on sampling, a copy of the questionnaire and a summary of the business characteristics of respondents, see Annex 1.

new provisions amongst respondents, and how it relates to their cost expectations. By consolidating all pieces of evidence we then assess the robustness of the different figures advanced by stakeholders.

Finally, in Section 4, we use responses to our survey to determine which policy tools available to the ICO would be most useful in assisting businesses to implement the proposed Regulation.

3.1 Overall expected costs and benefits

The European Commission's Impact Assessment estimates that the proposals will lead to a net reduction in administrative burdens for business in the EU of €2.3 billion (£2.0 billion) per year. This entails a saving of €2.9 billion (£2.5 billion) from the harmonisation of data protection laws across EU Member States, less a cost of €580 million (£496 million) for businesses to demonstrate compliance to the new laws, and a cost of €20 million (£17 million) from notifying authorities of personal data breaches. The Impact Assessment does recognise that there will be additional compliance costs arising from the DPO and DPIA requirements, but does not attempt to quantify these costs and excludes them from its overall net benefit figure.

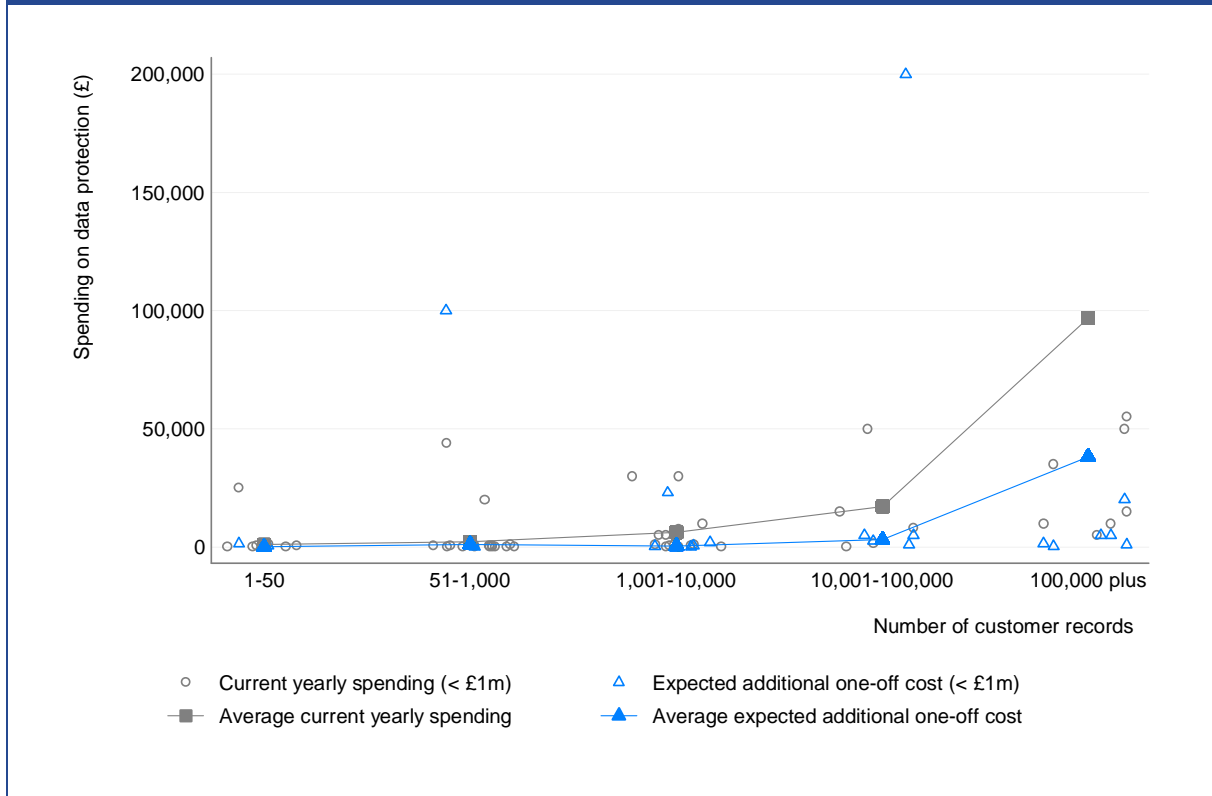
Following the Commission's publication of the new data protection legislative proposals and ensuing Impact Assessment, the Ministry of Justice (MoJ) launched a 'Call for Evidence' that ran from 7 February to 6 March 2012. This consultation sought information on the expected impact of the draft Regulation and Directive directly from affected stakeholders in the UK. In light of the responses received, the MoJ carried out its own Impact Assessment with the aim of presenting a "fuller summary of the costs and benefits of the proposals and their wide-ranging impacts on affected sectors of society in the UK."²² The MoJ study draws specific cost figures from a variety of sources (including the EC impact assessment, the Call for Evidence, surveys and other studies) and weights them to reflect the UK business demography, so as to deliver overall cost and benefit ranges. According to the MoJ study, the Regulation is expected to lead to a net cost to business of between £80 million and £320 million per year. The expected net present value of the Regulation to the UK over the next fourteen years is -£2.1billion (including costs and benefits to individuals and the public sector as well as to businesses).

According to responses to our own business survey, a large majority of companies are unable to quantify current spending on data protection (82%). When asked about expectations of future spending (once the new Regulation comes into force) an even larger proportion of respondents (87%) are unable to provide any estimates (both for one-off adjustment costs and additional yearly compliance costs). Of the remaining 13%, 8% expect zero additional costs.

In contrast, one company expects to spend an extra £5 million to adjust to the proposed Regulation and, on top of that, £1 million per year to comply. Figure 1 and Figure 2 below illustrate current and expected future spending on data protection in relation to the volume of records held by the company. The connected solid points reflect mean spending for the whole sample, while the hollow shapes represent spending of individual firms.

²² MoJ (2012), *Impact Assessment*, p.5

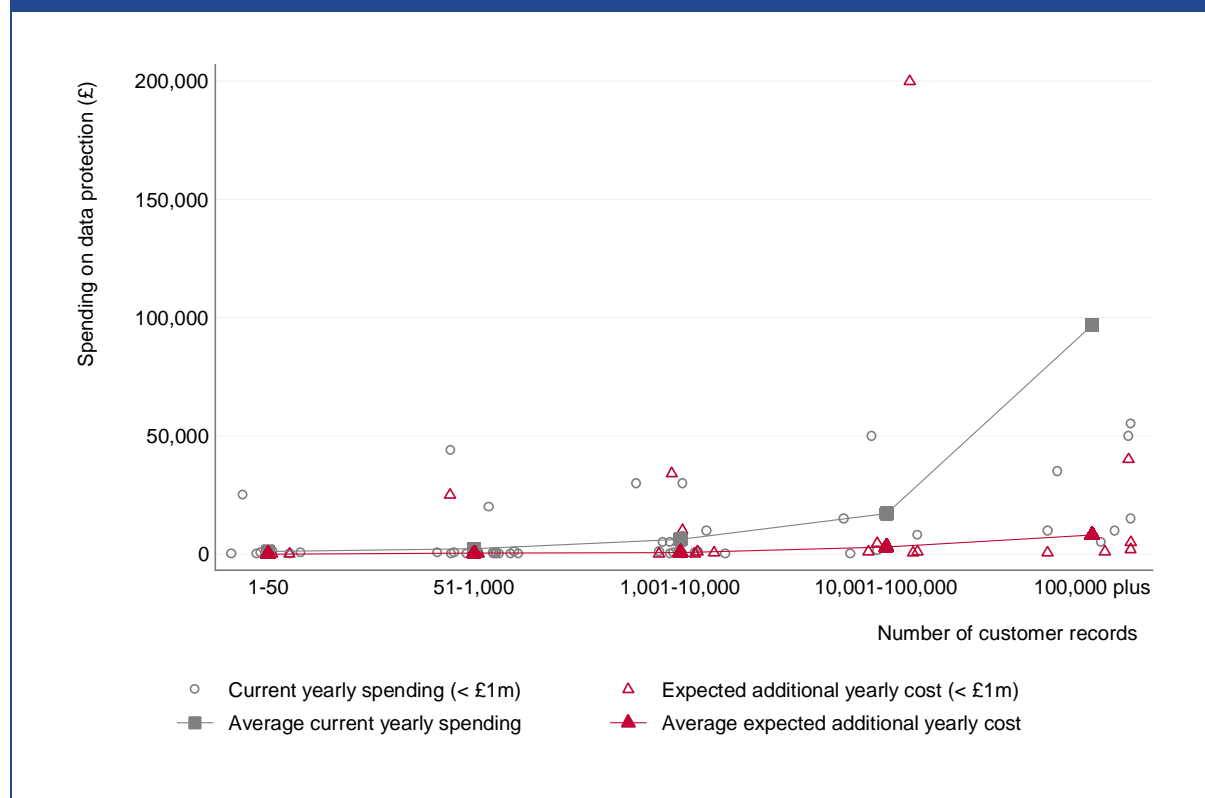
Figure 1: Current yearly spending and expected additional one-off costs, by number of customer records held



Note: Mean current spending and additional expected cost are calculated using the entire sample of respondents. The hollow gray circles and blue triangles represent the corresponding individual data points. We restrict these observations to positive spending under £1 million to aid visibility.

Source: London Economics

Figure 2: Current yearly spending and expected additional ongoing costs, by number of customer records held



Note: Mean current spending and additional expected cost are calculated using the entire sample of respondents. The hollow gray circles and red triangles represent the corresponding individual data points. We restrict these observations to positive spending under £1 million to aid visibility.

Source: London Economics

Aside from the clearly large variability in cost expectations among businesses, two points emerge from these figures:

- **current and expected additional spending on data protection increases substantially for firms holding more than 100,000 records of personal data; and**
- **average costs (current and expected) are driven by a small number of large observations.**

This suggests that the evidence put forward by stakeholders needs to be judged in relation to the fact that firms who a) are able to put a figure on their data protection expenditure and b) possess large volumes of personal data are not representative of the UK business population as a whole. Therefore studies that derive aggregate cost estimates for the UK under the assumption that figures reported by such firms reflect the average cost to business may be misleading. We will explore this possibility in more detail in the following subsections.

3.2 Costs and benefits of key provisions

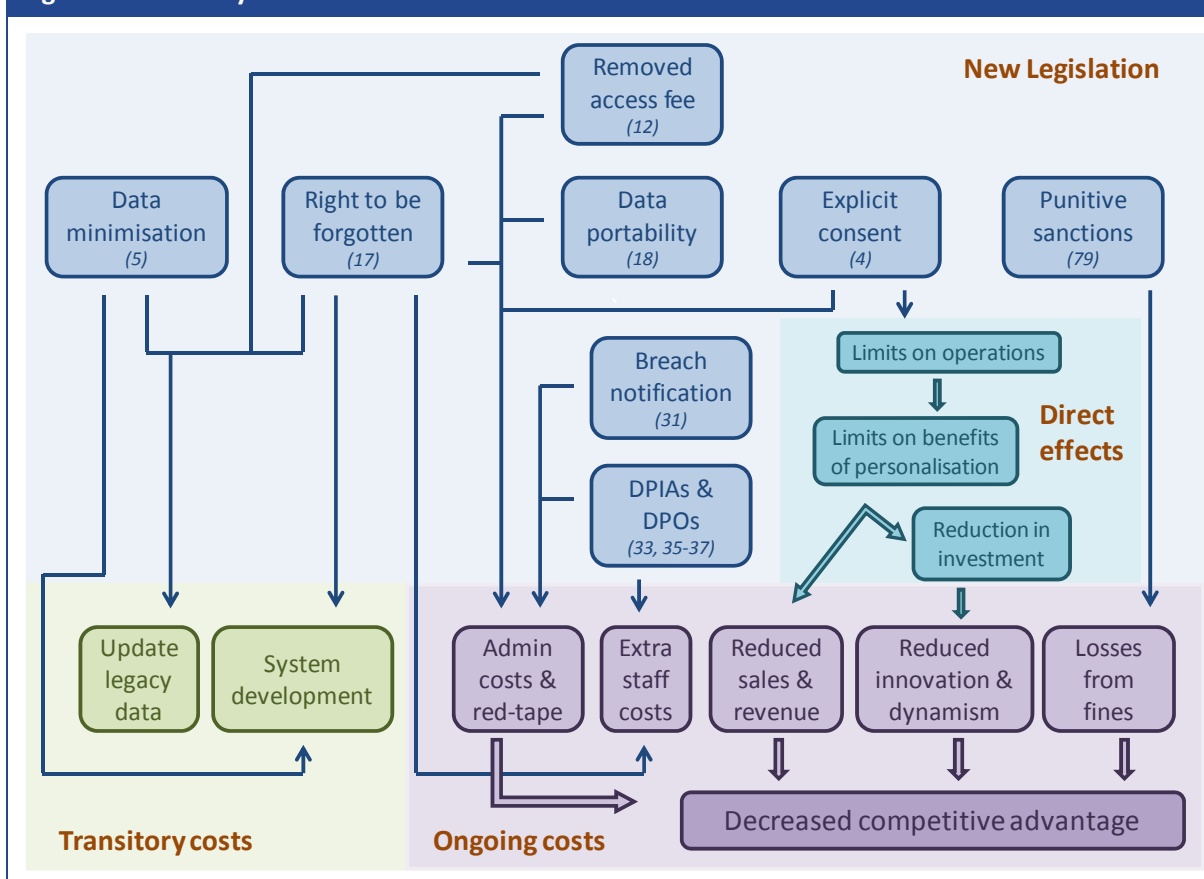
Responses to MoJ's Call for Evidence and insights from its Impact Assessment, combined with commentaries by the Confederation of British Industry (CBI) and evidence collected by the Direct

Marketing Association (DMA) have informed us of which articles in the new Regulation are likely to have the most significant impact on UK business. These include:

- lack of clarity around some definitions (Article 4);
- higher standard of consent (Articles 4(8) and 7);
- data minimisation (Article 5);
- new and strengthened rights for data subjects (Articles 12, 17 and 18);
- breach notification within 24 hours (Article 31);
- data protection impact assessments prior to risky processing operations (Article 33);
- obligation to appoint a data protection officer (Articles 35-37); and,
- imposition of large fines for failure to comply (Article 79).

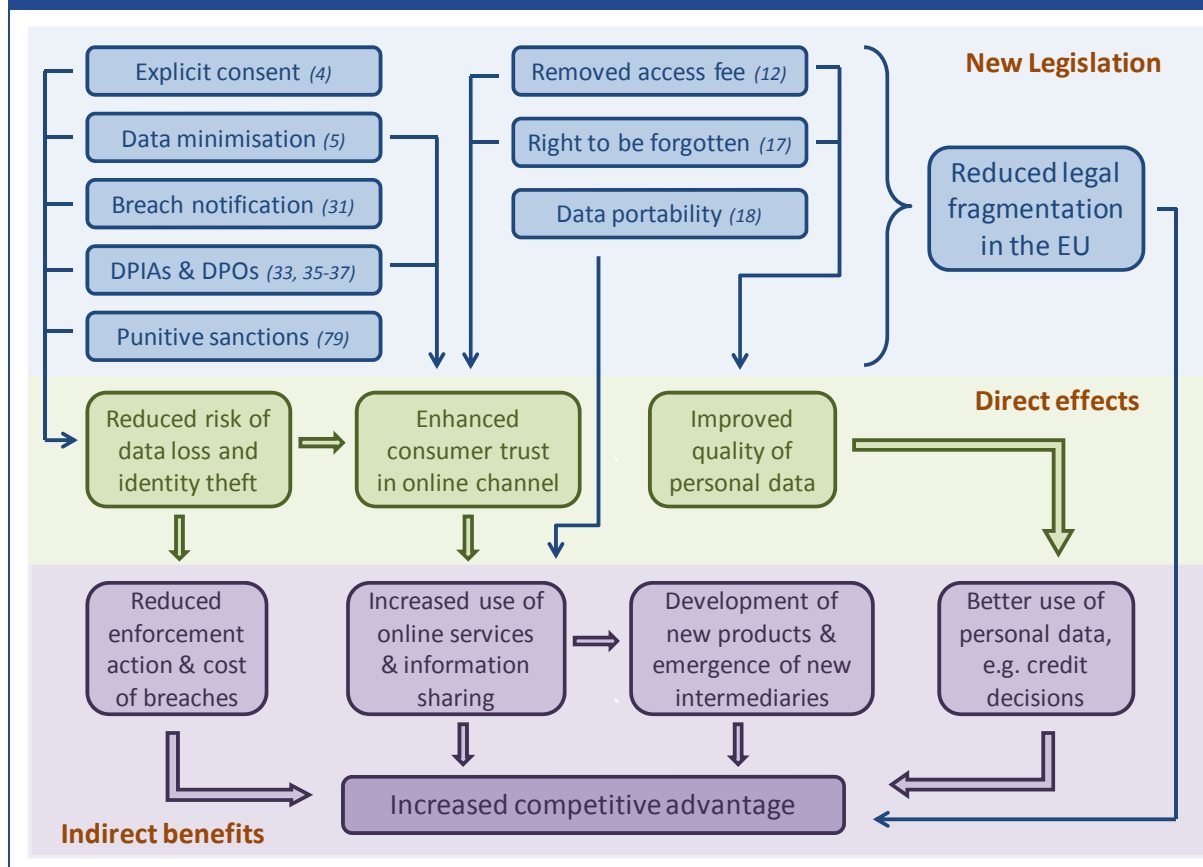
In the following subsections, we examine each of these provisions in detail, and review the existing evidence provided by stakeholders on its associated costs and benefits to business. A summary of the mechanisms through which these provisions are expected to affect businesses in the UK is provided below (Figure 3 and Figure 4).

Figure 3: Summary of costs



Source: London Economics

Figure 4: Summary of benefits



Source: London Economics

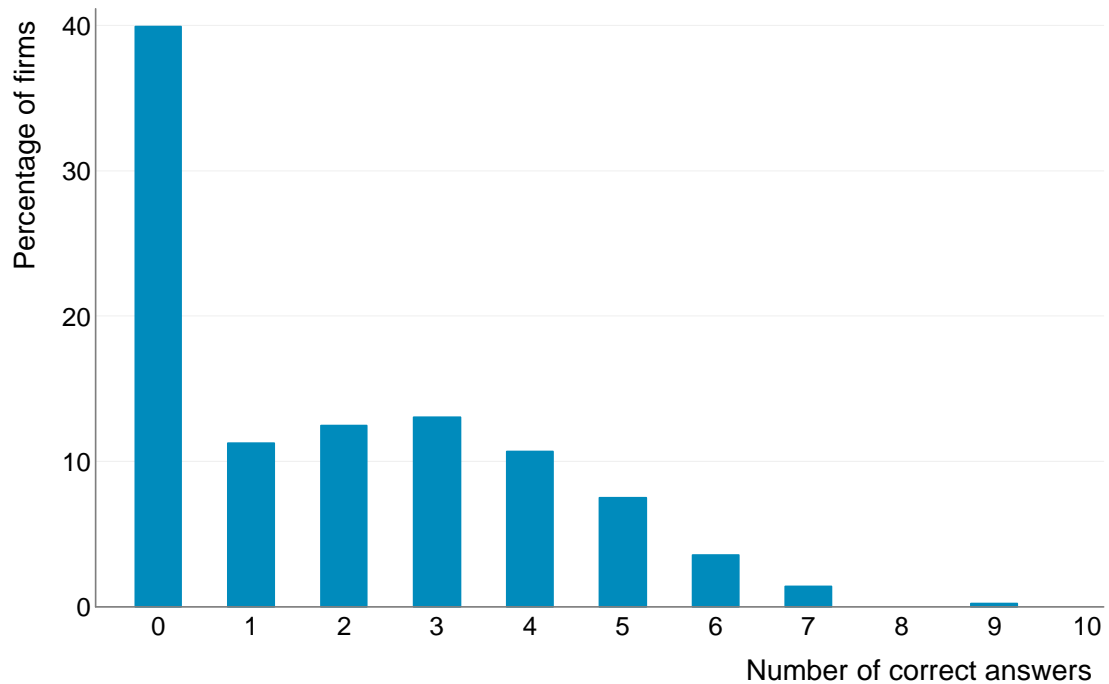
The drivers of cost expectations

What emerges from our review of the evidence is that many UK businesses expect the repercussions of the new Regulation to be large. One approach to evaluating the validity of these claims is to determine what drives companies' conjectures of future costs associated with data protection regulation. On these grounds, we investigate which business characteristics are associated with systematically higher cost expectations, and whether this differs for companies with different levels of knowledge of the proposed Regulation.

In our business survey, for each of the key provisions listed above, we ask respondents to select one of three possible definitions: one of these responses reflects the current legislation (*status quo*); one the new Regulation (*correct*); and one a more restrictive but fictitious definition (*incorrect*).²³ Figure 5 illustrates the distribution of correct answers across firms. As shown below, 40% of companies that participated in our survey have inaccurate knowledge of all 10 provisions considered. None accurately describe all 10 provisions.

²³ For the full list of questions and answers, see Annex A1.2.

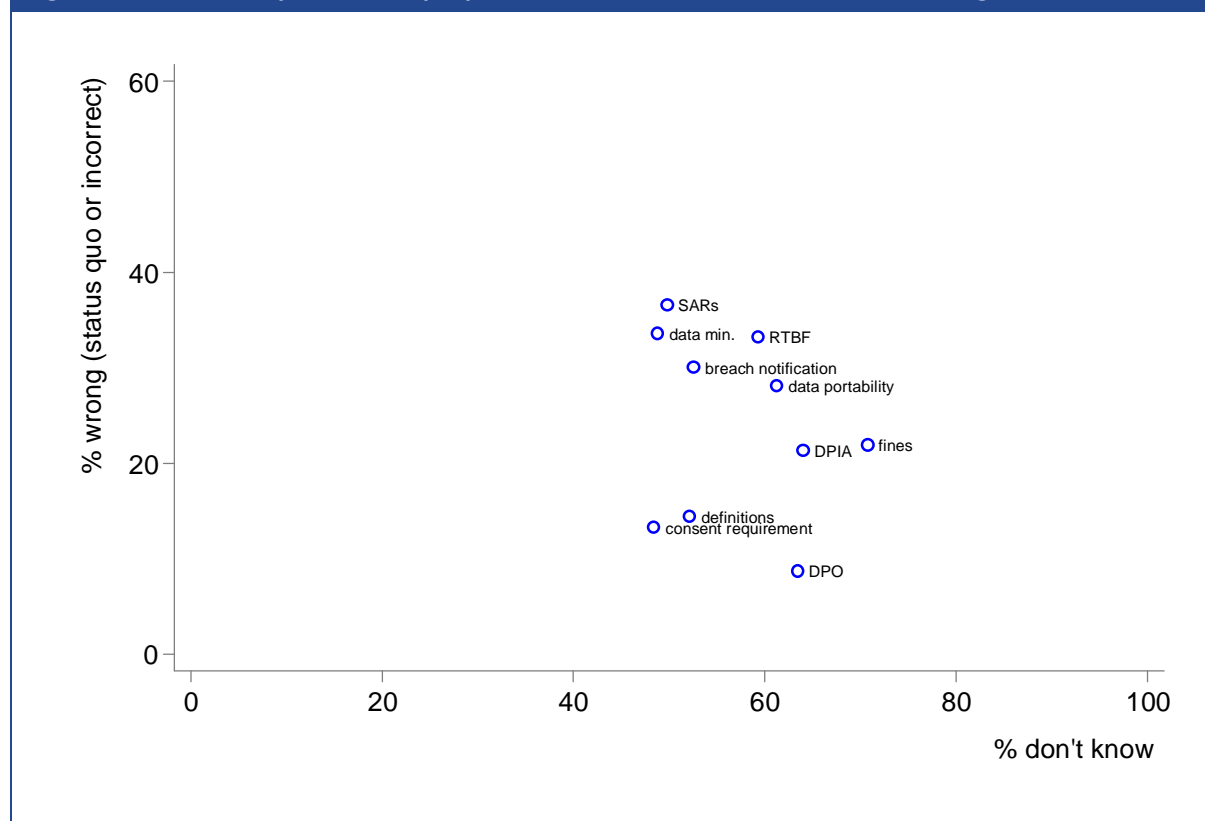
Figure 5: Number of correct answers on knowledge of provisions



Source: London Economics

A comparison between the proportion of survey respondents who gave a wrong answer to the questions about the content of the provisions (i.e., they either named the status quo instead of the proposed measure or a fictitious stricter measure) or recorded a 'don't know', shows the scale of the uncertainty: at least 48% (consent requirements) and up to 71% (administrative fines) of respondents report they don't know the scope of the provision in the EC proposals, while between 9% (DPO) and 37% (SARs) get the content of the proposals wrong.

Figure 6: Uncertainty about the proposed measures (% don't know vs % wrong)



Note: “wrong” answers are answers where respondents identified either the status quo or a fictitious (stricter) provision as the proposed measure.

Source: London Economics

In summary, the survey evidence suggests that a majority of companies in the UK do not have a clear grasp of how data protection regulation will change once the EC proposals are enforced. Moreover, this lack of understanding persists for companies that hold over 100,000 records of personal data, and presumably dedicate a significant amount of resources to data collection, processing and storage.²⁴

It is important to note, however, that this lack of understanding is not necessarily the result of ignorance on the part of firms, but may also be driven by the complexity of the proposed Regulation and the persistent uncertainty about the meaning and implications of some of its provisions.

We use the total number of correct answers per firm described above to construct a measure of the firm’s ‘knowledge’ of the provisions and incorporate this variable into a model that relates a number of firm-specific variables with cost expectations.²⁵ Due to the inability of most firms to

²⁴ The distribution of correct answers remains unchanged when we distinguish between companies holding less than 100,000 records of customer or third party data and those that hold 100,000 and above. See Annex A1.3.3.

²⁵ We develop the model described here in an iterative procedure, progressively refining it by eliminating insignificant variables. For instance, once one accounts for the level of risk of harm from data security concerns, size of firm, number of records held and types of records held become superfluous and are excluded to improve precision of the model.

quantify expected costs numerically, we use a categorical measure of expected costs, on a scale from 1 (*no additional costs*) to 5 (*substantial additional costs*). Of the factors considered as potential drivers of cost expectations²⁶, two stand out:

- the extent to which firms derive large benefits from holding personal data; and
- the extent to which firms risk considerable damage from breaches of security or concerns over data security.

This is to be expected – companies that derive the greatest benefit from holding data will typically process and store data as a core part of their business, and as a result, incur higher costs from updating legacy data, developing new IT systems and ensuring compliance.

Interestingly, the combined effect of high benefits from holding data and greater knowledge of the proposed Regulation is to lower expected additional cost. This means that amongst companies that derive value from holding personal data, those that have a better understanding of what the new Regulation will entail report systematically lower expected costs than those who do not. This suggests that, to some extent, fear of excessive burdens from complying with the new legislation may be a result of misunderstanding or misinterpretation of the provisions, and the degree to which they differ from current law.

In the following subsections we replicate a similar analysis for each individual provision.

3.2.1 Definitions (Article 4)

The vast majority of respondents to the MoJ's Call for Evidence on the Proposed EU Data Protection Legislative Framework are concerned over the lack of clarity in some definitions used in the proposed Regulation. In particular, stakeholders are still unclear about the status of indirect identifiers (e.g. IP addresses, cookies), which, rather than being linked to a person, identify a device.

Respondents from the IT industry find that broadening the definition of personal data to include indirect identifiers such as IP addresses may inhibit businesses from providing certain services.

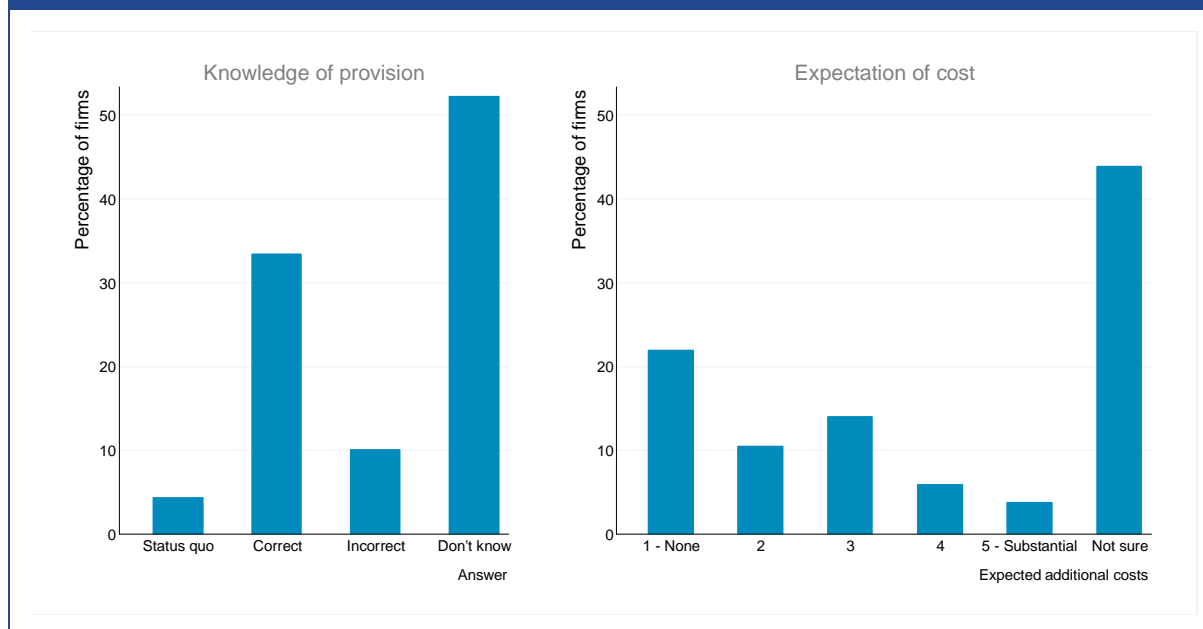
The Federation of Small Businesses (FSB) are concerned that the new definitions of "personal data", "processing" and "controller" will increase the remit of data protection, capturing more businesses and scenarios within the legislation and, as a result, increasing burdens on their business process and procedures. Moreover, the new legislation would affect even firms that do not handle data as an important part of their business.

As is apparent in the figure below, over half of the businesses that took part in our survey are unsure of how the proposed Regulation extends the definition of personal data. This corroborates the sense of vagueness of the provision that is expressed in the MoJ's Call for Evidence. A third of respondents, nonetheless, correctly understand this provision. This is the second highest proportion of correct answers out of all the provisions we consider. As we will see in the following

²⁶ A full description of the variables considered and the regression output is available in Annex 0.

subsections, this provision is also characterised by a larger than average proportion of ‘no additional cost’ responses.

Figure 7: Distribution of respondents’ answers to the question on the definition of personal data (left); and distribution of related cost expectations (right)



Source: London Economics

As before, we performed an econometric analysis of the predictors of expected additional cost related to the extended definition of personal data. Unlike our model of overall cost expectations, where ‘knowledge’ captures the firm’s breadth of knowledge of all relevant provisions, here we focus on knowledge of this particular provision alone²⁷. We find that the most significant predictor of cost expectations is, again, the firm’s risk of damage from data security issues.

Interestingly, firms that employ staff with data protection responsibilities and have accurate knowledge of this provision tend to report higher expected costs. One explanation for this is that companies that already employ staff, whose core responsibilities relate to data protection, handle larger amounts (and potentially more sensitive types) of data. It is for these companies that the extension of the definition of personal data may pose restrictions on business activity. Because they have an accurate understanding of the new provision (as opposed to the general lack of clarity described by most stakeholders), they will recognise how the extension of the definition of personal data will affect their activities – i.e. more than the average firm.

3.2.2 Consent and conditions for consent (Articles 4(8) and 7)

Responses to the MoJ’s Call for Evidence indicate a number of concerns amongst businesses about the higher standard of consent, defined as “explicit,” and about the conditions for consent, which place the burden of proving consent on the data controller. More than half of the respondents felt

²⁷ Again the model for individual provisions was developed by iteration, progressively eliminating insignificant factors. As such, the total number of correct answers is excluded from the model.

that this would require data controllers to give data subjects an “opt-in” for their personal data to be collected.

In a digital environment, explicit consent requirements impose practical difficulties. Requiring data controllers to provide data subjects with an opt-in to the processing of their personal data (where this processing is based on their consent) is particularly onerous when data controllers must also gain consent for placing cookies on users’ equipment (Privacy and Electronic Communications Regulation 2003). The Internet Advertising Bureau (IAB) is concerned that making the online experience more cumbersome will generate “consent-fatigue”²⁸. This may actually undermine data protection concerns by leading them to opt-in as a matter of routine rather than encouraging informed consent.

Moreover, according to evidence submitted to the MoJ²⁹, the implementation costs involved in complying with Article 7 (on the burden of proof) – namely, printing, storing and producing a physical copy of the data subject’s acceptance to a statement of consent – would be a considerable burden, especially for SMEs.

Consent requirements are particularly sensitive for direct marketing and e-commerce firms. The FSB notes that a significant cost for e-commerce businesses will be to adapt their websites to ask for consent to gather data. Case study evidence gathered by the Direct Marketing Association (DMA) reveals how the formulation of the legislation which is currently in place would lead to cuts in profitability, increased costs and even staff losses. The DMA estimate that in 2011, £14.2 billion was spent on direct marketing, which generated, directly or indirectly, 530,000 UK jobs.³⁰ Restrictions in this market are thus likely to be costly to the UK economy. The Internet Advertising Bureau (IAB) estimates that the new Regulation may cost UK businesses up to £633 million per year in lost advertising revenues as firms reduce spending on online advertising. Using survey evidence from a sample of 600 UK companies, the DMA estimates the overall cost to business of stricter consent requirements to be £47 billion, due to the inability to target consumers directly.

There may also be costs in terms of reduced investment in internet start-ups, which would particularly harm the ICT sector. Booz & Co. carried out a survey of 189 angel investors and 24 venture capitalists in the US to investigate the impact of changes in privacy regulation on the decision to invest in advertising technology companies.³¹ They find that introducing an opt-in requirement for the collection of personal data reduces the number of investors in advertising technology by 65%.³² Moreover, by restricting the ability to generate sales revenues or develop new digital media applications through direct marketing, the provision would constrain innovation and dynamism in the industry.³³

²⁸ IAB (2012)

²⁹ MoJ (2012), Summary of Responses, p. 14.

³⁰ DMA (2012), pp. 5, 9

³¹ Though the study uses a survey of investors in the US, a significant amount of their investments were directed to high-tech companies in the EU.

³² Le Merle et al (2012)

³³ DMA (2012), p.12

Preliminary findings on the cost of higher consent standards to business are summarised in the table below.

Table 1: Estimated costs of provisions on consent by business activity

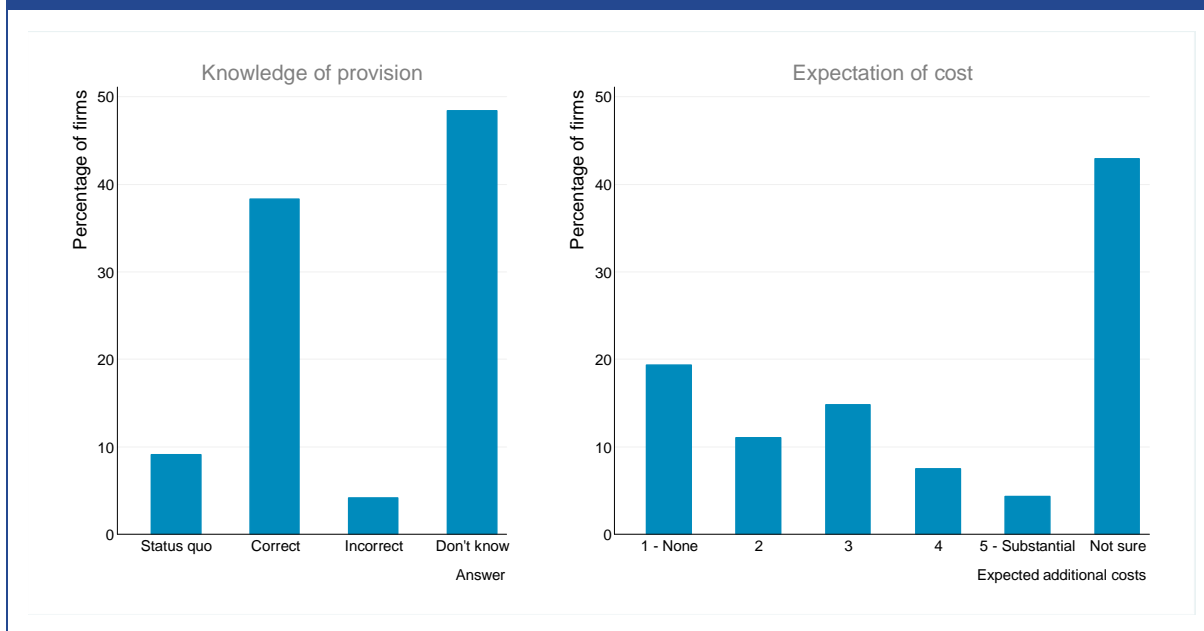
Business activity	Transitional costs	On-going costs
<i>Financial services</i>	Reformulating existing customer databases could cost anywhere between £100,000 and £500,000. [DMA – Financial service organisation]	The requirement for explicit consent could lead to an inability to market to existing customers thereby losing revenue of approximately £6 million. [DMA – Financial service organisation]
<i>Data services</i>	Reviewing and updating legacy data to comply with the Regulation would cost approximately £6 million. [DMA – Global data company]	Explicit requirements for consent would lead to annual losses in revenue of £1 million. [DMA – Global data company]
<i>Direct Marketing & Digital Advertisement</i>		Additional costs generated by administration from the right to be forgotten, explicit consent for data processing and the training of a data protection officer would lead to estimated extra costs of £50,000 - £75,000 per year. [DMA – Global marketing service provider] The explicit consent requirement could lead to a 50% drop in turnover and a loss of 26 jobs. [DMA – List broking company] The proposals as drafted may cost UK businesses up to £633 million in lost advertising revenue. [IAB]
<i>E-commerce Retailers</i>	Adaptation of websites. [FSB]	
<i>ICT</i>		Requiring data subjects to opt-in before any data is collected reduces the pool of investors in advertising technology start-ups by 65%. [Booz&Co]
<i>Membership Organisations</i>		The requirement for explicit consent would make fundraising via marketing impossible. An extra £90,000 would have to be found to cover increased telemarketing staff numbers. [DMA – Charity membership organisation]
<i>Other Business Services</i>		The explicit consent requirement would lead to a 50% drop in business. [DMA – Bureau cleaning service]
Total UK businesses		Average cost of £76,000 per year per SME which translates to £47billion per year to all UK businesses [DMA – Putting price on direct marketing]

Source: London Economics

While the implementation of explicit consent will no doubt pose difficulties to direct marketers and online advertisers, the cost figures illustrated above may be misleading. In particular, the DMA's prediction of a £47 billion loss in revenue per year reflects a loss in the total value of direct marketing to the UK economy – i.e. it assumes that this provision will wipe out the direct marketing business entirely.

It's hard to believe that enforcing the explicit consent requirement will eradicate this market completely, no matter how burdensome for businesses. This being said, there is a legitimate need for greater clarity as to what exactly constitutes explicit consent. Our survey analysis, in fact, reveals that 48% of companies are unsure of what the higher standard of consent entails. Moreover, even though a good proportion of companies give the right answer (38%), this does not prove that these companies understand the substance of the new definition – i.e. how/if the term “explicit” differs from the term “unambiguous”.

Figure 8: Distribution of respondents' answers to the question on consent requirements (left); and distribution of related cost expectations (right)



Source: London Economics

Benefits and risks associated with holding data are again among the strongest predictors of expected additional cost of the explicit consent requirement (see Annex A1.4). Interestingly, for this particular provision, the factor that has the largest positive impact on expected costs is the presence of staff whose core responsibilities involve data protection. As before, this could reflect the greater dependence on large quantities of personal data by firms that employ data protection staff.

Business benefits

Business may derive certain indirect benefits from the implementation of higher consent standards. Specifically, shifting the burden of proof of consent on businesses is likely to reduce the risk of data loss or misuse. The result is that there will be an overall reduction in costs arising from litigation and fines. Additionally, enhanced consumer trust in data controllers may spur increased usage of the online channel.

The business benefits engendered by greater consumer trust (more users, more data, more accurate information) are potentially very large. However, to our knowledge, no conclusive evidence exists to show that the growth of e-commerce can be further accelerated by strengthening consent requirements. The evidence that portrays consumers as reluctant

participants in an online market that offers insufficient levels of control over personal information is difficult to judge when seen against the background of strong growth in e-commerce in both EU and non-EU jurisdictions. Moreover, some evidence suggests that consumers that feel more in control of their personal data disclose more of it (“paradox of control”³⁴), thereby potentially leading to overall greater risk of harm through data loss, as well as potential adverse effects on market structure (reduced competition due to the trust advantage of incumbents/big brands). The question of business benefits clearly warrants more research.

3.2.3 Data minimisation (Article 5)

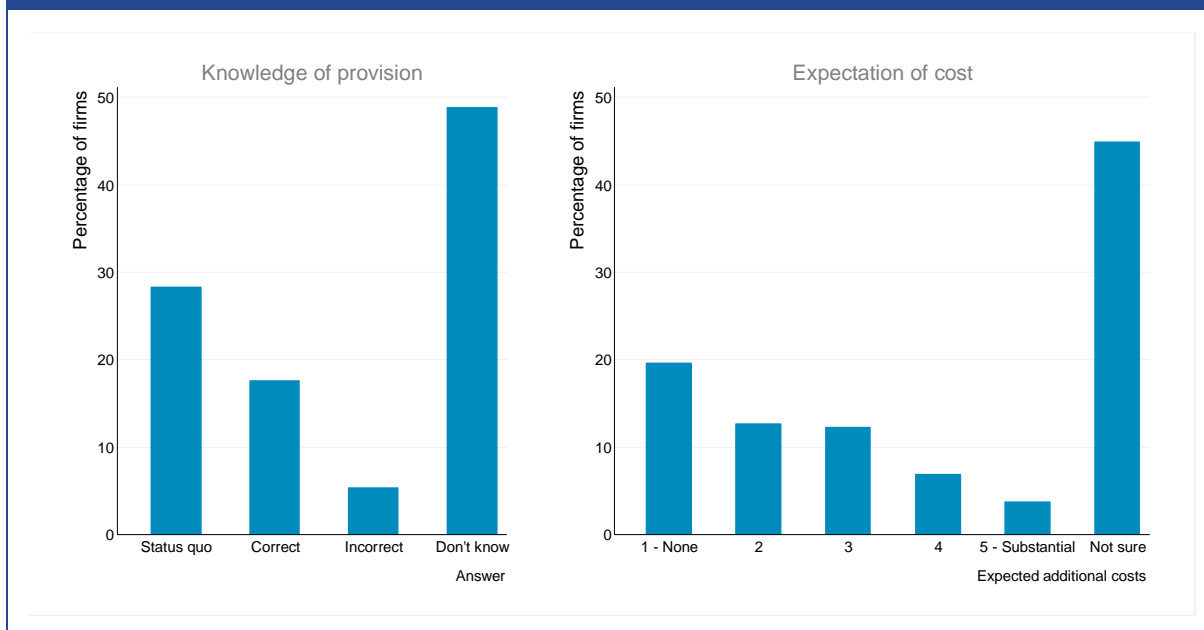
The requirement that personal data be “limited to the minimum necessary” was welcomed by data protection advocates, who find that it will reassure consumers that only the minimum indispensable amount of their personal data will be used by data controllers to provide a service. Increased trust in service providers clearly benefits business.

However, data controllers who responded to the MoJ’s Call for Evidence indicated that the financial impact of ensuring compliance of their existing databases with the proposed regulation is potentially very large (up to £10-15 million for a media sector company alone).

Unlike the preceding two provisions, in the case of data minimisation the second largest category of answers is *status quo*, meaning a large proportion of firms believe the new provision to require what is actually already prescribed by current law. In fact, the new provision does not diverge considerably from the current requirement whereby personal data must be “adequate, relevant and not excessive in relation to the purposes for which they are collected”. Here, large adaptation costs may be exaggerated by companies that overestimate the additional requirement of this provision relative to the current legislation.

³⁴ See e.g. Tucker (2010); Brandimarte et al. (2010).

Figure 9: Distribution of respondents' answers to the question on data minimisation (left); and distribution of related cost expectations (right)



Source: London Economics

The most interesting result from our estimation of the drivers of cost expectations related to data minimisation is that companies that are unsure of the provision's meaning (*don't know*) report systematically higher additional costs relative to the base (*status quo*). This provides additional support for the claim that poorer knowledge of the new provisions is associated with higher-than-average cost expectations.

3.2.4 Rights of the data subject (Articles 12, 17 and 18)

The practical and financial challenges that have sparked the most discussion by stakeholders are those that relate to provisions that strengthen the rights of data subjects. Notably,

- Art. 12: abolishment of the fee for subject access requests (SARs);
- Art. 17: the right to be forgotten and to erasure; and,
- Art. 18: the right to data portability.

Some stakeholders are concerned that these measures may have the unintended effect of distorting consumer behaviour. In the case of fee abolishment, there is the concern that this will lead to an increase in frivolous and/or vexatious requests, putting strain on resources and budgets. Similarly, business respondents feel that the provision on data portability may induce consumers to swamp companies with requests to have their personal data made available to them in an agreed format for reuse, putting severe strain on their resources (particularly in the case of SMEs). The *right to be forgotten* is widely considered over-ambitious and impractical; moreover, in an environment where data can be replicated and divulged in seconds it is found to be misleading and place “unrealistic expectations” on data controllers.

Table 2 below summarises predictions of costs and benefits that are associated with the prescribed articles, as expressed by a variety of stakeholders.

Table 2: Costs and benefits of provisions strengthening data subject rights for business

Business activity	Transitional costs	On-going costs	Business benefits
Data Services	<p><i>Articles 12 & 17:</i> A one-off cost of £500,000 for system development to meet right to be forgotten, privacy by design and removal of subject access fees. [DMA – Data service provider for retailer]</p> <p><i>Articles 17 & 18:</i> Data portability and right to be forgotten could require a one-off system development at a cost of £100,000. A cost of up to £5 million for data already collected but could not be used if the Regulation is retrospective. [DMA – Global data company]</p>		<p><i>Article 18</i> Benefits to data service providers if portability encourages the rise of new information services. [MoJ – Call for Evidence]</p>
Marketing	<p><i>Article 17:</i> The cost of updating the CRM system would run into the thousands of pounds. [DMA – B2B telemarketing and digital marketing company]</p>	<p><i>Articles 4, 17 & 35:</i> Additional costs generated by administration from the right to be forgotten, explicit consent for data processing and the training of a data protection officer would lead to estimated extra costs of £50,000 - £75,000 per year. [DMA – Global marketing service provider]</p>	
Financial Services	<p><i>Article 17 & 18:</i> Cost of changes to IT systems and services. [MoJ – Call for Evidence]</p>	<p><i>Article 12:</i> Increased volume of SARs + no fees to help pay for costs of SARs, estimated at £100-£500 per SAR. Cost of providing extra information (e.g. how long data will be stored for), more quickly.</p> <p><i>Article 17:</i> Additional costs of dedicating staff to this task; difficulty in tracking deletion and rectification; and, obligation to demonstrate. [MoJ – Call for Evidence]</p>	<p><i>Article 12:</i> If people are encouraged to correct their personal data, better credit decisions will be made about individuals. [MoJ – Call for Evidence]</p>
ICT		<p><i>Article 18</i> “Mandating a single format for data transfer will require technology providers to</p>	<p><i>Article 12</i> 73% of individuals surveyed by Populus said ‘the ability to withdraw my data’ would</p>

	change other aspects of their products and services, which may result in less functionality, less diversity and worse overall user experience.” [Microsoft]	make them more comfortable with sharing information. [MoJ – Impact Assessment] Article 18 Benefits may arise if portability encourages the rise of new information services. [MoJ – Call for Evidence]
Total UK businesses	Article 12 £12-37 million [MoJ – Impact Assessment]	

Source: London Economics

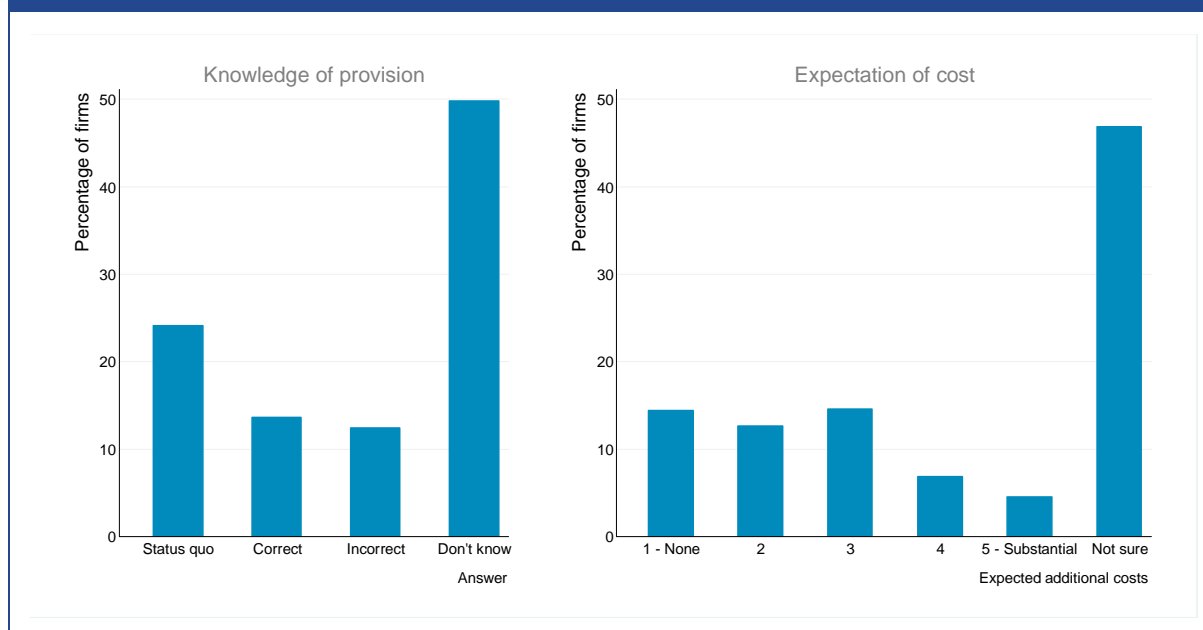
Subject Access Requests (SARs)

According to the MoJ’s Impact Assessment, the additional cost to business of removing fees for data subjects to access their data depends solely on the cost of responding to a SAR and on the increase in number of SARs. The loss in income from the fee itself is more than offset by the removed cost of administering the fee. The MoJ estimates that removing the £10 fee will increase the number of SARs by 25-40%.³⁵ The estimated cost of responding to a SAR ranges £50-£100 per request (though respondents to the MoJ’s Call for Evidence from the financial services sector reported costs of £550-£650 per request). Using the loss estimates of £50-£100, the MoJ estimates that the cost to business of Article 12 will range from £12 million to £37million, depending on the extent of the increase in SARs.

As with data minimisation, a sizeable portion of respondents to our business survey fail to identify the subtle difference between the current legislation and what is intended by the new provision (see Figure 10). Specifically, about a quarter of companies do not recognise the abolishment of the fee for SARs (as opposed to current law which allows fees that are not “excessive”). Nearly half the companies in the sample cannot predict how this provision will affect their business.

³⁵ These figures are based on studies in which fees were introduced in Ireland and Ontario, leading to a reduction in FOI requests (Office of Information Commissioner, 2005; and Frontier Economics, 2006).

Figure 10: Distribution of respondents' answers to the question on subject access requests (left); and distribution of related cost expectations (right)



Source: London Economics

The econometric analysis relating knowledge of the provisions and other firm characteristics to cost expectations shows a consistent pattern for the provisions on subject access requests, right to be forgotten, data portability, breach notifications and data protection impact assessments: the predictor that has the largest effect on cost expectations is the presence of staff with data protection responsibilities³⁶.

Right to be forgotten

It is the European Commission's political aim to give internet users a greater degree of control over the availability and use of their personal data. The right to be forgotten fits into this agenda. Under current law, individuals are granted the right to demand "rectification, erasure or blocking of data"³⁷ that is inaccurate, incomplete or unlawfully processed. Moreover, personal data can be retained "for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"³⁸.

In a society based on increasingly personalised services, where every piece of information can be argued to be relevant, this limitation is rather flexible. Data controllers have an ample margin of appreciation in determining for how long retaining personal data serves a legitimate purpose. Once consent is granted, the current legal framework does not provide individuals with substantial, real-time control over their personal data. The proposed right aims to address this by shifting the balance of power from data controllers to data subjects.

³⁶ All regression results are shown in Annex 1.

³⁷ Directive 95/46/EC, Article 12(a).

³⁸ Directive 95/46/EC, Article 6(e).

More controversially, the proposed Regulation would make data controllers responsible for the publication of personal data by third parties. This combined with the imposition of high sanctions in the event of non-compliance, may incentivise companies to “opt for deletion in ambiguous cases, producing a serious chilling effect.”³⁹ There is widespread concern that this “may encourage pre-emptive censorship and curb innovation”⁴⁰ in digital services. Though difficult to quantify, such an impediment to innovation may pose a significant burden on businesses, particularly on internet-based start-ups.

Another concern is that an increased perception of control over publication of personal information encourages consumers to disclose more sensitive information (the so-called “privacy paradox”). Behavioural research⁴¹ shows that, even if people have no control over who accesses or uses their personal information, having control over its *publication* increases their willingness to reveal private information. Moreover, individuals are more likely to answer intrusive questions and reveal sensitive information if they are in control of whether it is published or not. Thus, granting consumers the right to be forgotten, which strengthens this feeling of control, may result in a “revelation of ‘too much’ private information”⁴², with the assurance that it can at any future date be erased and “forgotten”. It may not be technologically feasible to erase all copies made by third parties and divulged on the web, or prohibitively costly for data controllers to do. If failing to abide by the obligation results in punitive fines then this could entail significant added burdens to business.

The right to be forgotten is associated with one of the lowest proportions of *correct* answers (7.5%) and a relatively even distribution of expected additional costs across the 1-5 scale.

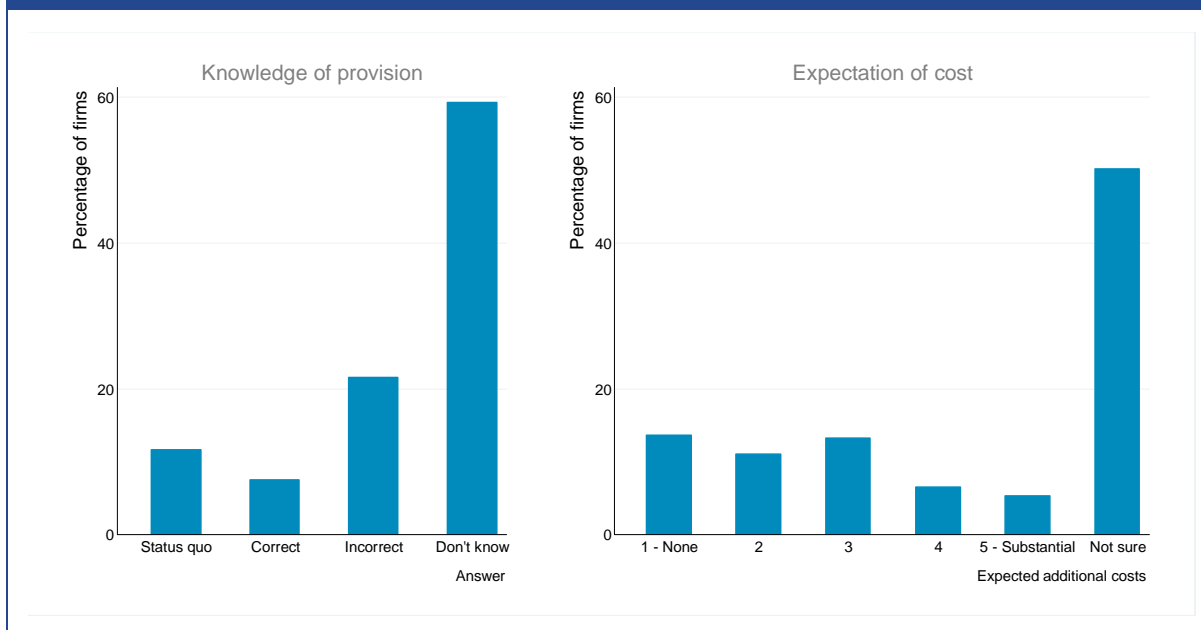
³⁹ Rosen (2012), p.91

⁴⁰ Graux et al. (2012), p.16

⁴¹ Acquisti et al. (2010)

⁴² Ibid., p.29.

Figure 11: Distribution of respondents' answers to the question on the right to be forgotten (left); and distribution of related cost expectations (right)



Source: London Economics

Data Portability

Article 18 of the proposed Regulation grants the data subject the right to obtain the following from the data controller:

- a copy of any personal data undergoing processing in an electronic format that is specified by the EC and that allows for further re-use; and
- the right to share that data with another controller.

In the UK, the Department for Business, Innovation and Skills (BIS) has already proposed introducing a similar scheme through its midata initiative. At the moment, midata (or analogous schemes) are adopted by organisations on a voluntary basis. However, BIS is exploring the possibility of making portability – the transfer of personal data from one firm to another upon the data subject's request – legally enforceable for firms in the same industry.⁴³ Hence, as noted in the MoJ's Impact Assessment, the additional costs and benefits to UK businesses of data portability as set out in the new Regulation will depend on (a) the extent to which the midata initiative is legally enforced; (b) the extent to which organisations already proactively offer such services; and, (c) the extent to which consumers will make use of this new right once the Regulation comes into force.

For instance, in the telecommunications industry, data portability allows consumers to seek the lowest price for a service by accessing all their information. Billmonitor found that switching to the most suitable phone contract would have saved consumers £5.98 billion in 2011.⁴⁴ By incentivising

⁴³ BIS (2012)

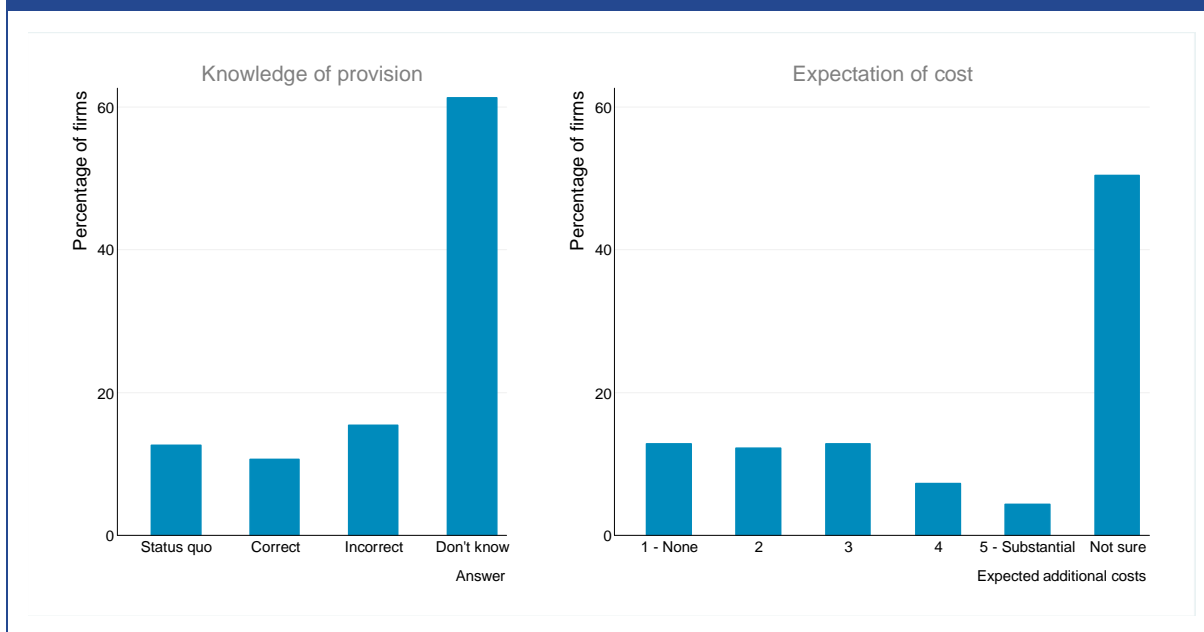
⁴⁴ Billmonitor (2012)

firms to compete on price, data portability leads to a number of indirect benefits including the development of new products and the emergence of new intermediary firms that help consumers use their data to find the most suitable tariff. The realisation of these benefits, however, requires consumers to actually exercise this right. Thus, the gain from introducing this data portability depends critically on the extent to which consumers will use their data.

In terms of our survey analysis, similar conclusions hold as with subject access requests and the right to be forgotten:

- there is widespread uncertainty amongst businesses in relation to the meaning of the provision; and,
- firms that process more data and are at greater risk of damage from security concerns expect above average implementation and compliance costs.

Figure 12: Distribution of respondents' answers to the question on data portability (left); and distribution of related cost expectations (right)



Source: London Economics

3.2.5 Breaches, sanctions, DPIAs and DPOs (Articles 31, 79, 33 and 35-37)

Other provisions which may pose an excessive financial burden on business activity include:

- Art. 31: notification of personal data breaches to supervisory authorities within 24 hours;
- Art. 33: performance of Data Protection Impact Assessments (DPIAs);
- Art. 35-37: mandatory employment of a data protection officer (DPO); and,
- Art. 79: administrative sanctions of up to 2% of annual turnover.

Though these provisions all share the benefit of deterring negligent or wilful misuse of data, thereby reducing overall ICO enforcement costs, they may impose very high costs on the business activity, particularly for small hi-tech data-intensive companies.

These costs are mildly attenuated by the removal of the general notification requirement, whereby data controllers must notify the supervisory authority of their processing activities. The ICO estimates its general notification fee income to be £15.5 million per year (54% of which is from the private sector)⁴⁵. Data controllers will also save the administrative burden of completing the annual notification form (though they will still be required to maintain documentation as prescribed by Article 28) which was estimated to cost £12.6 per data controller by PwC in 2005. This implies an additional cost saving to UK businesses of £2.4 million.

A summary of estimated costs and benefits is provided in Table 3.

⁴⁵ However, assuming that different sources of funding will be used to maintain the ICO's activities, money no longer spent on notification fees does not necessarily represent net savings for businesses.

Table 3: Costs and benefits of provisions on breach notifications, administrative sanctions and DPIA/DPO requirements

Business activity	Transitional costs	On-going costs	Business benefits
Marketing		<p><i>Articles 35-37:</i> Additional staff training would cost £7,600 per year. [DMA – B2B telemarketing and digital marketing company]</p> <p><i>Articles 35-37:</i> DPO requirements for a large research organisation they could easily add over £5 million annually to the cost of doing business. The additional process steps and delays that would take a toll on business performance are not included in this figure. [Market Research Society]</p>	<p><i>Article 31</i> Mandatory notification may encourage data controllers to implement more robust security measures, thus avoiding further enforcement action and reducing the cost of breaches. [MoJ – Call for Evidence]</p> <p><i>Article 35-37</i> Employing DPOs may aid compliance, reduce infringements and lead to fewer data breaches, increasing consumer confidence and reducing the risk of ICO sanctions/enforcement actions. [MoJ – Call for Evidence]</p>
Financial Services		<p><i>Articles 35-37:</i> Small businesses that have to designate a DPO, as their core activities are based on processing personal data (e.g. financial and insurance companies) would be hard hit. The appointment of such an officer could cost around £30,000–£75,000 annually. [FSB]</p> <p><i>Article 79:</i> HSBC had global revenues of around £63 billion in 2010, thus a 2% fine, if applied in full, could cost the company in the order of £1.2bn. [CBI]</p>	<p><i>Article 31</i> Mandatory notification may encourage data controllers to implement more robust security measures, thus avoiding further enforcement action and reducing the cost of breaches. [MoJ – Call for Evidence]</p> <p><i>Article 35-37</i> Employing DPOs may aid compliance, reduce infringements and lead to fewer data breaches, increasing consumer confidence and reducing the risk of ICO sanctions/enforcement actions. [MoJ – Call for Evidence]</p>
Business Services		<p><i>Article 31:</i> Estimated average notification cost of £172,000 per breach in the UK. [Symantec/Ponemon]</p> <p>Taking 2010/2011 figures for breaches reported to ICO as base, if the number of minor unreported breaches is similar, mandatory notification will increase costs by £104 million (603 x £172,000). [MoJ – Call for Evidence]</p> <p><i>Articles 35-37</i> Estimated cost of £50,000 per year to employ a DPO per company. If 50% of large data controllers (5,900 in the UK) already have a member of staff fulfilling this role, the additional cost</p>	<p><i>Article 31</i> Mandatory notification may encourage data controllers to implement more robust security measures, thus avoiding further enforcement action and reducing the cost of breaches. [MoJ – Call for Evidence]</p> <p><i>Article 35-37</i> Employing DPOs may aid compliance, reduce infringements and lead to fewer data breaches, increasing consumer confidence and reducing the risk of ICO sanctions/enforcement actions. [MoJ – Call for Evidence]</p>

	will be £147m per year. [MoJ – Call for Evidence]	
ICT/ Research	Article 35-37 Costs of employing a DPO are likely to be higher for small firms who undertake large amounts of data processing such as hi-tech start-ups and medical research organisations. [MoJ – Call for Evidence]	
Total UK businesses	Article 31 Total annual cost of reporting security breaches <ul style="list-style-type: none"> ▪ SMEs: £20-£55 million ▪ Large firms: £11-£76 million ▪ Total: £31-£131 million Articles 33 Total annual cost of carrying out DPIAs <ul style="list-style-type: none"> ▪ Micro: £14 million ▪ SMEs: £54 million ▪ Large firms: £14 million ▪ Total: £81 million Articles 35-37 Total annual cost of employing DPOs <ul style="list-style-type: none"> ▪ SMEs: £182 million ▪ Large firms: £47 million ▪ Total private: £229 million [MoJ – Impact Assessment]	Articles 31, 33, 35-37 and 79 Total annual savings from reduced personal data breaches as a result of breach notification, sanctions, DPOs and DPIAs <ul style="list-style-type: none"> - SMEs: £34-£68 million - Large firms: £25-£56 million - Total: £58-£124 million Removal of general notification requirement £2.4 million [MoJ – Impact Assessment]

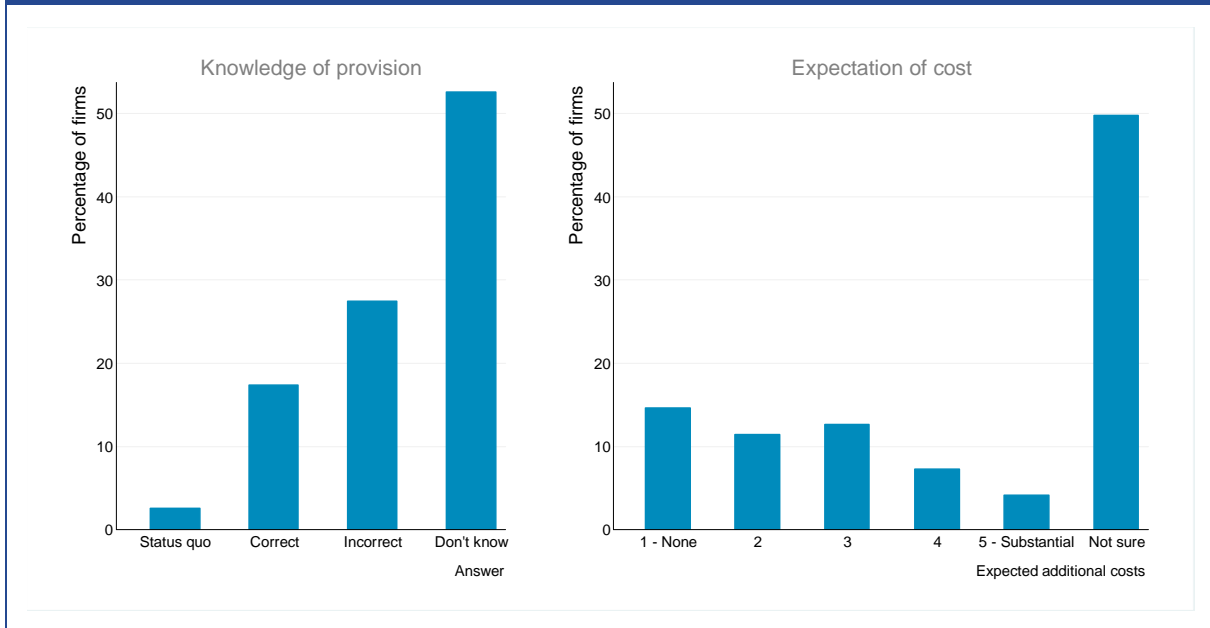
Source: London Economics

Notification of breaches

What emerges from our survey analysis is that more than a quarter of respondents believe the proposed breach notification requirement to be more restrictive than it actually is. In other words, companies mistakenly assume that *all interested parties* (i.e. including data subjects) must be notified of a breach of personal data without undue delay, when in fact the new Regulation will require only the supervisory authority to be notified. Again, half of our sample is unsure of how this will affect their costs of doing business. No additional insight is yielded by our econometric analysis⁴⁶.

⁴⁶ See Figure 40, Annex 1.

Figure 13: Distribution of respondents' answers to the question on breach notification (left); and distribution of related cost expectations (right)

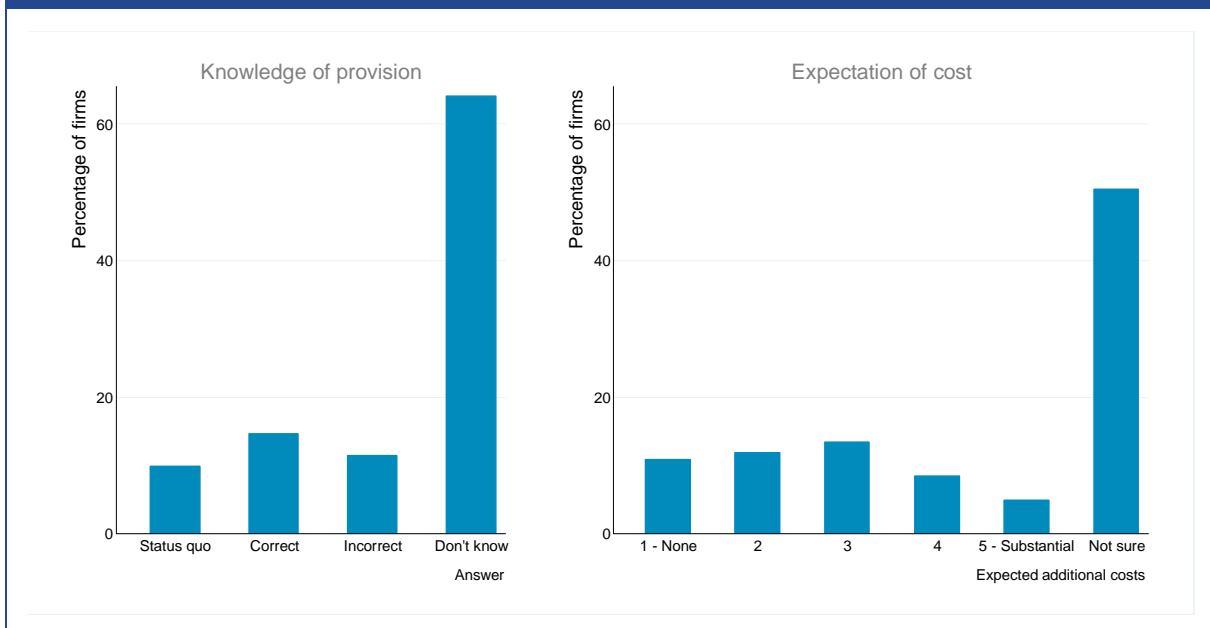


Source: London Economics

Data protection impact assessments

Almost two thirds of the companies that participated in our survey are unsure of what the provision on data protection impact assessments prescribes. Expected additional costs are fairly evenly distributed, with a small majority selecting an intermediate cost level on a scale from 1 to 5.

Figure 14: Distribution of respondents' answers to the question on DPIAs (left); and distribution of related cost expectations (right)



Source: London Economics

The only factor that has a significant and positive impact on cost expectations (see Annex 1) is risk of harm to business from breaches in security or other data security concerns.

Data Protection officers

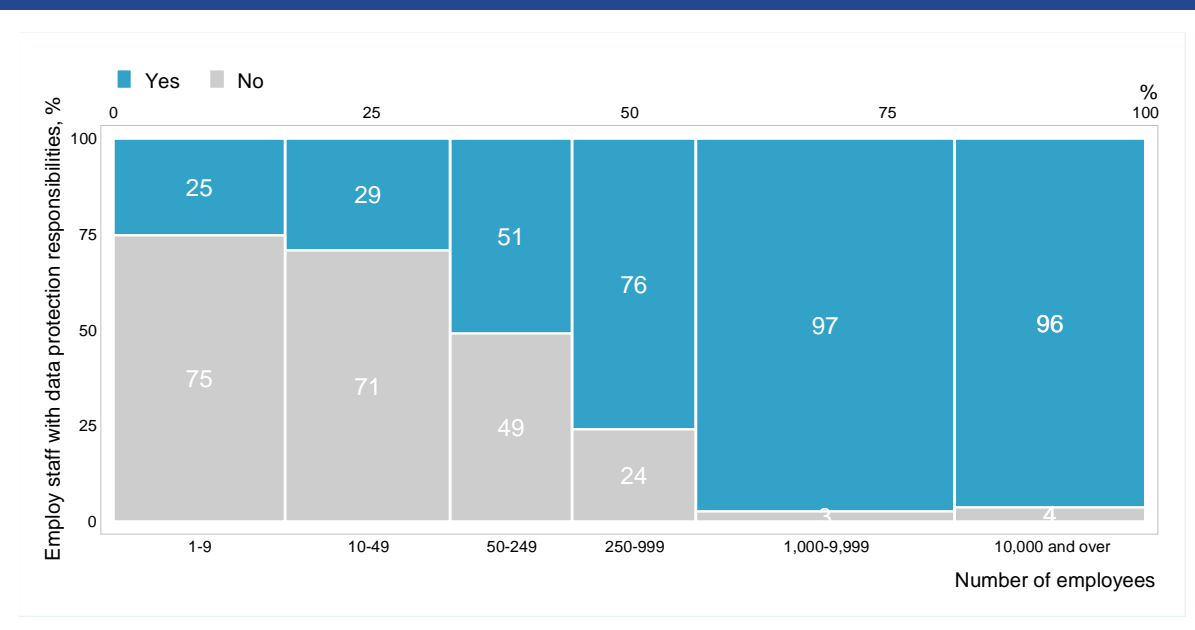
Our survey reveals three important facts that relate to the employment of staff whose core activities involve data protection compliance:

- the vast majority of companies with over 250 employees already employ staff with a job role focused on data protection compliance (Figure 15);
- the vast majority of companies who keep more than 100,000 records already employ staff with a job role focused on data protection compliance (Figure 16); and
- companies that perceive greater risk for their business from breaches of data security or concerns about data security are more likely to have employees with a job role focused on data protection compliance (Figure 17).

These facts suggest that the majority of firms to which this provision applies are already satisfying the requirement and need not expend significant additional resources to comply with the new Regulation. This is in stark contrast with some of the cost estimates displayed in Table 3. One market research company, for instance, reports an added £5 million annually to the cost of doing business.

This discrepancy is consistent with another finding that emerges from our survey, namely that already employing staff with a job role focused on data protection compliance is not associated with lower expectations of costs from the requirement to employ a DPO (Figure 18). Moreover, almost half of the respondents are not sure about the costs associated with the requirement to employ a DPO.

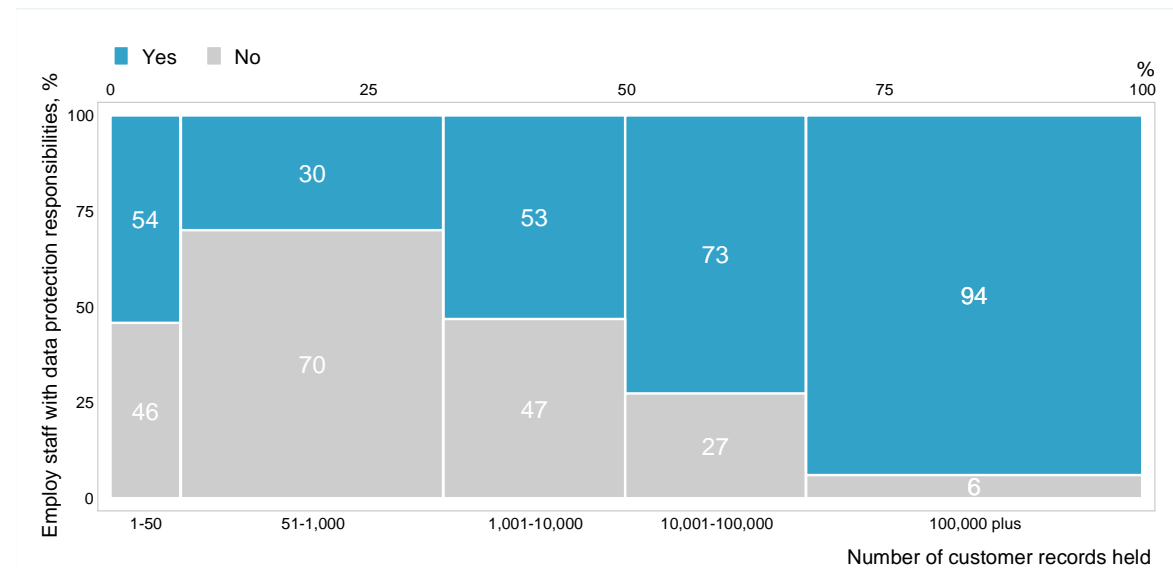
Figure 15: Likelihood of employing staff with data protection responsibilities given firm size



Note: The proportion of firms that employ staff with data protection responsibilities increases according to the number of employees in the firm.

Source: London Economics

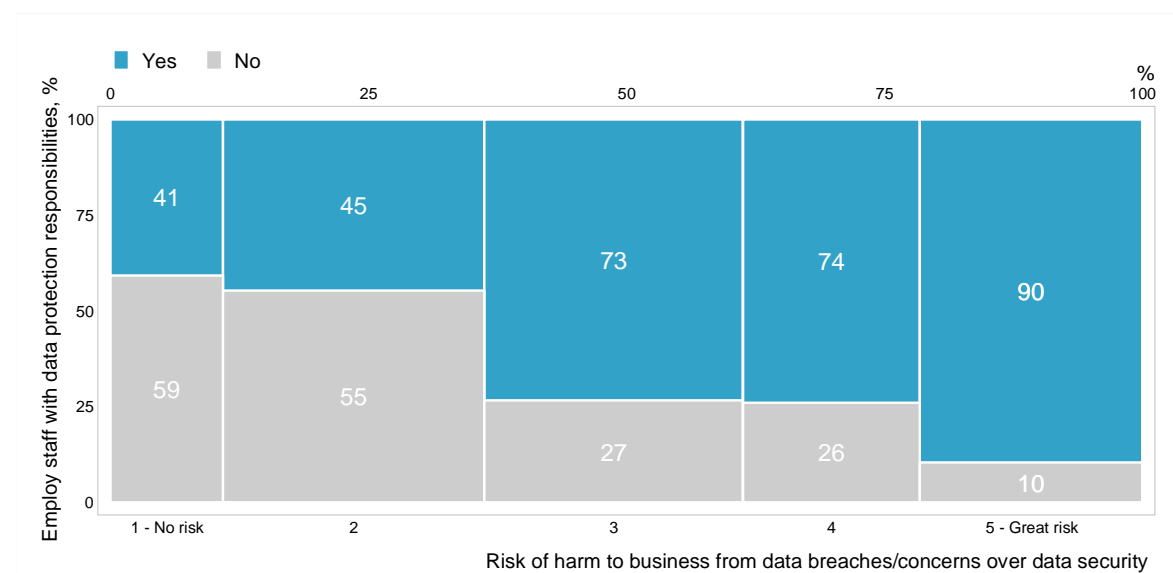
Figure 16: Likelihood of employing staff with data protection responsibilities given number of customer records held



Note: The proportion of firms that employ staff with data protection responsibilities increases according to the number of customer records held by the firm.

Source: London Economics

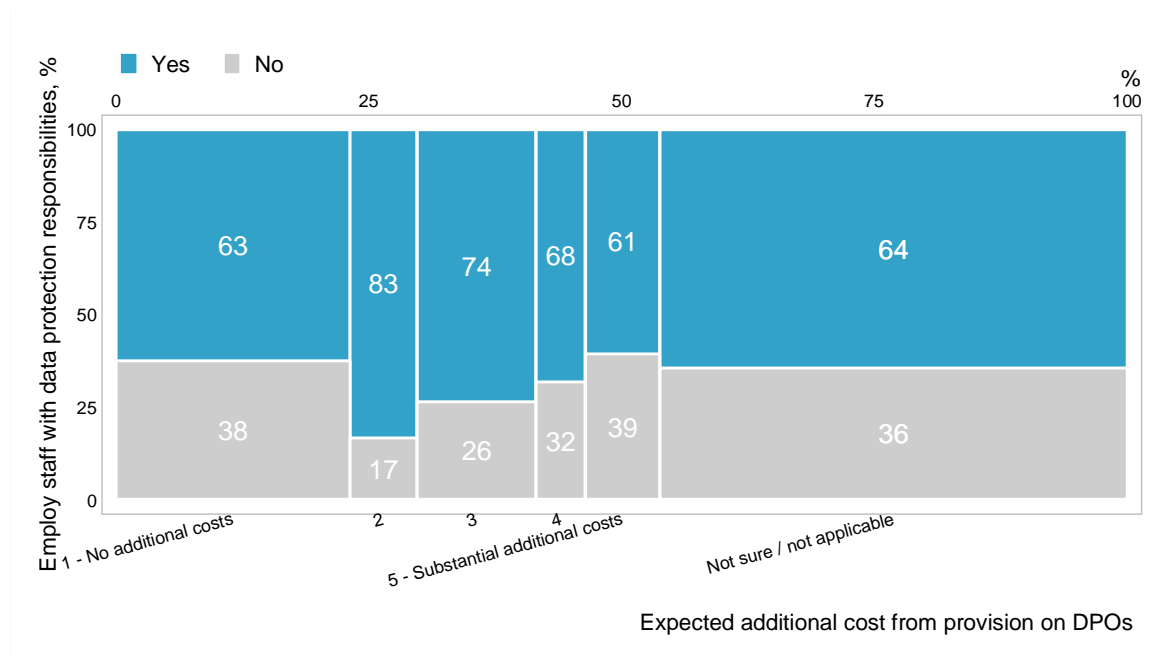
Figure 17: Likelihood of employing staff with data protection responsibilities given risk of harm to business from data security concerns



Note: The proportion of firms that employ staff with data protection responsibilities increases according to the degree of risk is perceived by the firm.

Source: London Economics

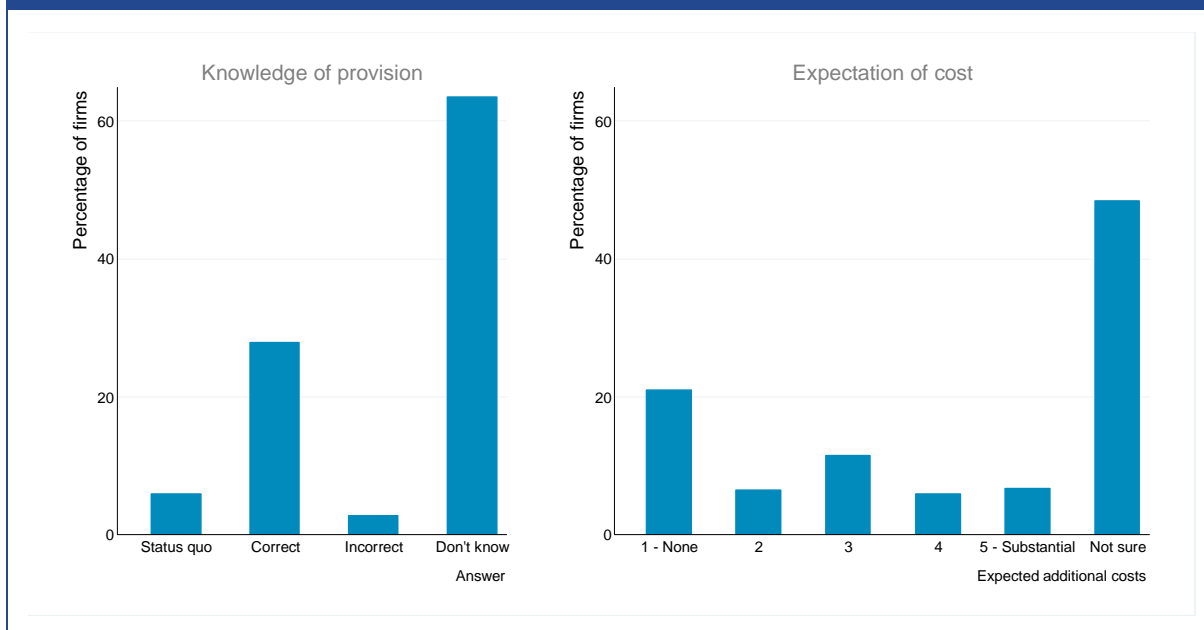
Figure 18: Proportion of firms that employ staff with data protection responsibilities and expectations of costs from DPO provision



Note: The proportion of firms that employ staff with data protection responsibilities is roughly flat across different levels of cost expectations.

Source: London Economics

Figure 19: Distribution of respondents' answers to the question on DPOs (left); and distribution of related cost expectations (right)



Source: London Economics

The arbitrary incorrect answer that we introduced as one of the possible descriptions of this provision is that companies in excess of 250 employees or whose core activities involve data processing must hire a *new* employee to cover the role of DPO. This was done precisely to verify whether much of the controversy around this provision is in effect driven by this overly onerous interpretation of the provision. In reality, companies need only appoint a DPO. As most companies for which this will become mandatory are already employing staff whose main concern is data protection, this provision should require at most limited retraining of such staff. In our model, while the confidence intervals are very wide, the estimated impact of misinterpreting the proposed Regulation as described above (i.e. the coefficient on *incorrect*) is positive and large in magnitude.

Administrative sanctions

Article 79 proposes the administrative fines for failure to comply with the Regulation, based on a three-tier fine system:

- Tier 1: up to €250,000 or 0.5% of annual global turnover (e.g. failure to comply with SAR);
- Tier 2: up to €500,000 or 1% of annual global turnover (e.g. failure to maintain correct documentation); and
- Tier 3: up to €1 million or 2% of annual global turnover (e.g. failure to designate a DPO).

Currently, the maximum fine that can be applied by the ICO is of £500,000 for the most serious breaches of the Data Protection Act. Under the new Regulation, the maximum penalties are not only considerably higher, but also relatively higher penalties can be applied to less serious breaches of security. As noted by the MoJ's Impact Assessment, sanctions are imposed "regardless of the harm caused" and the ICO is not given the discretion to withhold from imposing a sanction in the event of a breach of the Regulation: "If the fine regime set out in the Regulation were

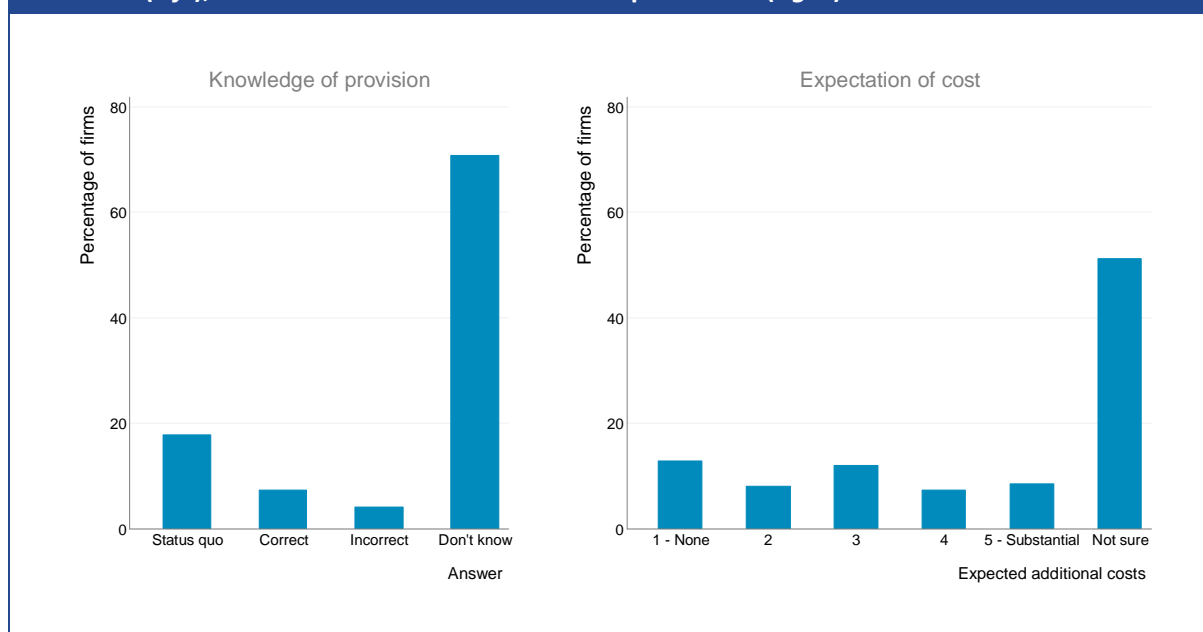
imposed in all cases where data controllers are found to be non-compliant, then the cost to business and the public sector would be considerable.”⁴⁷

Setting fines that are too high induces firms to misallocate resources by spending more than is necessary on data protection rather than other areas. In the extreme case, this can drive the marginal firm out of business. The difficulty in quantifying these indirect costs is reflected in the lack of estimates of monetised costs for this particular provision in the existing evidence.

Our survey analysis shows that, of all the provisions considered, the one on administrative fines receives the largest share of unsure answers relating to the description of the provision in the survey. This is also the provision that receives the largest proportion of expected *substantial additional costs* (8.5%).

Our regression analysis shows that incorrect interpretation of the provision (whereby punitive fines of 2% of annual turnover must be applied in all instances of infringement of the Regulation) is associated with a significantly higher cost expectation relative to companies that expect the new provision to maintain the status quo.

Figure 20: Distribution of respondents’ answers to the question on administrative sanctions (left); and distribution of related cost expectations (right)



Source: London Economics

Enhanced protection of personal data

The 2012 edition of Infosecurity’s series of Information Security Breaches Surveys (of UK firms) finds that the incidence of breaches is at an all-time high, with almost half of all large firms and a tenth of small companies reporting a “breach of data protection laws or regulation”⁴⁸ over 2011-

⁴⁷ MoJ (2012) *Impact Assessment*, p.29

⁴⁸ Infosecurity and PwC (2012), p.10

2012. By implementing the provisions described in this subsection, data controllers should see a reduction in the amount of personal data that is lost or misused. In turn, this is expected to positively impact firms by reducing business disruptions, financial losses (from investigation, compensation and possibly revenue leakage), and reputational damage. Based on evidence from the same survey, the MoJ Impact Assessment estimates the reduction in breaches to save UK businesses £58 million to £124 million per year (see Table 3).

Focusing on reputation losses only, a study conducted by Acquisti, Friedman and Telang (2006) estimated the market reaction to the following types of privacy incidents:

- poor security practices;
- hacker attacks;
- insider attacks;
- computer or data thefts;
- loss of data or equipment; and
- other incidents such as the illegal sale or handling of individual data.

The study found a moderately negative, statistically significant cumulative drop in share prices per privacy incident of close to -0.6% on the day following the event, which equates to an average loss of approximately €7.4 million (£6.4million) in market value (based on US data). In general, this market reaction is of the same order of magnitude of reactions to similar announcements involving reputational damage (or gain). These (Jarrell and Peltzman, 1985; Chatterjee et al., 2001; Im et al., 2001; Dos Santos et al., 1993; Hendricks and Singhal, 1997) are also shown in Table 4 overleaf.

There is some evidence that security breaches involving personal data are more damaging to companies than other security breaches: Campbell et al. (2003) find that security breaches in which personal data was accessed had a significant impact on a company's stock market valuation, while the effect of incidents that did not involve personal data was insignificant. Among privacy breaches, those that involve financial data tend to result in larger share price reactions as might be expected, given the value of the information and including the effect of liabilities arising from legal claims in the future.

Table 4: Summary of studies on market reaction to security breaches

Classification of study	Authors	Time period	Number of events	Compound share-price reaction (%)
Impact of data breaches on share price	Acquisti, A., Friedman, A., and Telang, R. (2006)	2000-2005	79	-0.58
Impact of vulnerability disclosures	Telang, R. and Wattal, S. (2004)	1999-2004	146	-0.65
Impact of security breaches on firms (personal data accessed)	Campbell, K., Gordon, L.A., Loeb, M. P. and Zhou, L. (2003)	1995-2000	11	-5.4
Impact of security breaches on firms (all security breaches)	Campbell, K., Gordon, L.A., Loeb, M. P. and Zhou, L. (2003)	1995-2000	43	-1.9*
Impact of security breaches on firms	Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004)	1998-2000	66	-2.1
Impact of security breaches on firms	Hovav, A. and D'Arcy, J. (2003)	1998-2002	23	Not significant
Comparison results: impact on share price of other types of announcements that affect reputation				
Impact of auto recall announcements	Jarrell, G. and Peltzman, S. (1985)	1967-1981	116	-0.81
Impact of auto recall announcements	Davidson, W. L. III and Worrell, D. L. (1992)	1968-1987	133	-0.68
Impact of IT investment announcements	Chatterjee, D., Richardson, V. J. and Zmud, R. W. (2001)	1987-1998	96	1.16
Impact of IT investment announcements	Im, K. S., Dow, K. E. and Grover, V. (2001)	1981-1996	238	Not significant
Impact of IT investment announcements	Dos Santos, B. L., Peffers, K. and Mauer, D. C. (1993)	1981-1988	97	Not significant
Impact of winning a quality award	Hendricks, K. B. and Singhal, V.R. (1997)	1985-1991	0	0.59

Note: *not significant at the 10% level.

Source: Acquisti et al. (2006); reviewed in London Economics (2010)

In addition to these direct consequences of reduced data breaches, there may be an indirect benefit to businesses if these provisions reduce fraudulent use of personal data.

A survey by YouGov and commissioned by internet infrastructure company VeriSign Inc. estimates that, in 2009, 12% of UK citizens were victims of online identity theft, resulting in a financial loss of £463 per victim.⁴⁹ Reducing personal data breaches should lessen the extent to which data is fraudulently obtained and used. The MoJ argues⁵⁰ that this will generate additional benefits to business if it encourages consumers to purchase goods and services that require them to share their personal information online. While it is hard to quantify this added benefit, survey evidence gathered by Populus reveals that, “losing control of personal information is the most significant concern for the public” in the UK.⁵¹ For the MoJ⁵², this indicates that there is scope for enhancing online privacy and thereby increasing consumer confidence in the digital market.

3.3 Second-order effects

The proposed data protection regulation will affect businesses by (a) creating a harmonised legal framework throughout all the Member States of the European Union; and (b) introducing administrative changes (reporting requirements etc.) that affect the way businesses operate.

3.3.1 Reduced legal fragmentation

Currently, data controllers that operate in more than one Member State incur the cost of complying with the laws of each Member State they operate in. One of the two key aims of the Regulation is to harmonise laws on data protection within the EU, thereby removing some of these costs and strengthening the Internal Market.

The European Commission estimates these costs to be €5,000 (£4,000) for every additional Member State a data controller operates in, incurred every five years (€1000 annually).⁵³ A Eurobarometer survey provides evidence on the number of firms in a country that operate in other EU Member States, and how many Member States each operates in. Using these figures and applying the same methodology as in the EC Impact Assessment, the MoJ estimate that the cost of legal fragmentation to UK business is £66 million per year. If one accounts for the fact that only 27% of businesses operating cross-border had paid for legal advice on data protection issues in other countries, then this estimate drops to £42 million.

Thus, while the new Regulation as drafted does not provide for full harmonisation, it does provide businesses with significant savings in terms of translation costs, legal validation work and other administrative costs that arise from legal fragmentation in the area of data protection.

Moreover, our survey analysis provides evidence of a clear positive relationship between the extent of benefits from holding personal data on customers and whether or not a company

⁴⁹ VeriSign (2009)

⁵⁰ MoJ (2012), Impact Assessment, p. 25.

⁵¹ Bartlett (2012)

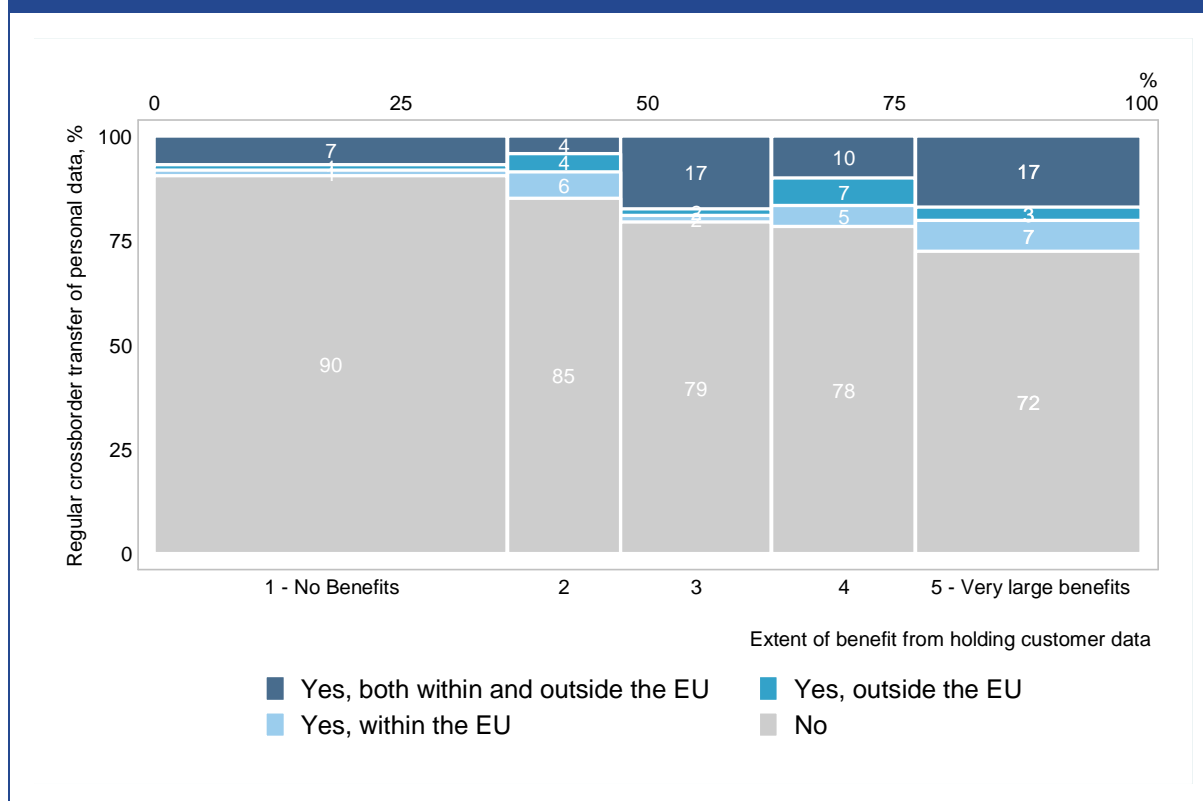
⁵² MoJ (2012), Impact Assessment, p. 26.

⁵³ EC SEC (2012) 72 final

transfers data across borders (Figure 21). This suggests that reducing legal fragmentation in the EU and facilitating the cross-border flow of personal information will be particularly advantageous to those same companies that expect to incur the highest costs of implementation and compliance.

While, thus far, we have ignored the implications of the provisions on international (i.e. extra-EU) transfers of personal data, it is worth noting that the reverse is true relative to within-EU transfers: by making international transfers of data more cumbersome and costly, the proposed Regulation is reducing the benefit these companies derive from holding personal data.

Figure 21: Benefit of holding customer data by firms that regularly transfer personal data crossborder



Source: London Economics

In order to get a better sense of how data controllers that operate in multiple countries expect their costs of business to change with the new Regulation, we extend the baseline model described at the beginning of the chapter to account for the regular cross-border transfer of personal data – within the EU, outside the EU and both.

Companies that regularly transfer personal data outside the EU as part of their core operations expect significantly higher overall costs, on average (Figure 35, A1.4).

3.3.2 Increased red-tape

One of the main criticisms of the EC's draft proposal is that it places too much emphasis on compliance paperwork, rather than results. Under Article 28, organisations are required to maintain documentation to prove that they are compliant, and provide it to their regulator upon

request. This paperwork, which is not a guarantee that the actual procedures in place in the organisation are up to standard, could impact significantly on SMEs that already employ good information handling practices.

Another obligation designed to demonstrate compliance requires organisations to obtain prior authorisation from the supervisory authority for processing (Article 34). This is viewed as disproportionate for companies seeking approval of outsourcing contracts, and at the same time could swamp the regulator with approval requests.

The new obligations will force organisations to change corporate policies and procedures, and implement new systems. Once the procedural changes are implemented, the added paperwork from communicating these changes to customers can also be very costly. The CBI presented estimates by a large financial services provider that the total cost of drafting, administering and sending out letters about policy changes amounts to £15 per customer, which adds up to millions of pounds for its total customer base. Additional costs for customer service to be able to deal with new queries arising from the policy changes could amount to another £100,000. It is clear that the cost of conveying information about policy changes to consumers rises with the number of consumers (although likely in a less than linear fashion, as larger organisations can be expected to be more efficient and experienced in administering such changes). The magnitude of the additional costs for business overall cannot be inferred from the example of a large financial services company, whose costs in relation to customer information requirements are likely to be affected by expansive sectoral regulation in addition to any additional general data protection.

The EC Impact Assessment estimates that the need to demonstrate compliance costs €200 (£160) per organisation, based on four hours of administrative work over a three year time span (or £53 per year per company). This figure is intended to capture all of the abovementioned administrative obligations on the data controller. Based on the EC methodology and the number of controllers registered in the UK, the MoJ estimates a total cost to business of £10 million per year. However, this figure is likely to be much higher if documentation needs to be updated more frequently than every three years. The MoJ give an upper bound estimate of the cost to UK business of £38 million per year (that assumes quarterly updating activity).

4 Priorities for the ICO

Box 5: Section summary

- 21% of firms in our sample have been in contact with the ICO on a previous occasion.
- Companies that handle **fewer** records of personal data are **more** likely to have had contact with the ICO in the past.
- Companies who had previous contacts with the ICO are much more likely to approach the ICO concerning the new Regulation.
- Overall, clear and concise guidance about the scope of the new provisions (changes from the status quo) available on the ICO's website is unambiguously the form of ICO support that is seen as most beneficial.
- ICO approved accreditation or certification schemes on specific areas of compliance are seen as the least beneficial.
- Implications for the ICO's business engagement strategy:

- The ICO should make information available and accessible through various channels (both on the website and through a manned contact point).
- An active information campaign should be used in parallel with and in support of measures to provide information on demand.
- Organisations in the areas of health and social work, financial and insurance services, public administration⁵⁴, as well as businesses in the broader services sector appear to suffer most from a combination of lack of knowledge of data protection rules and potential risk from data protection breaches.

Part of the ICO's brief was to provide recommendations about practical support and guidance the ICO could provide to businesses in the implementation of the most challenging articles, that will also deliver practical benefits for citizens. To address this research aim, we concluded our business survey with a number of questions relating to the company's history of contact with the ICO and the types of assistance it would find most useful to adjust to the new Regulation in the future. The evidence from the survey gives indications as to which types of businesses may be fruitfully targeted by ICO support and what type of support may be needed by different types of businesses.⁵⁵

4.1 Evidence on businesses' relationship with the ICO

With respect to businesses' relationship with the ICO, three interesting facts stand out from the analysis of the responses to the questions (Figure 22 and Table 5):

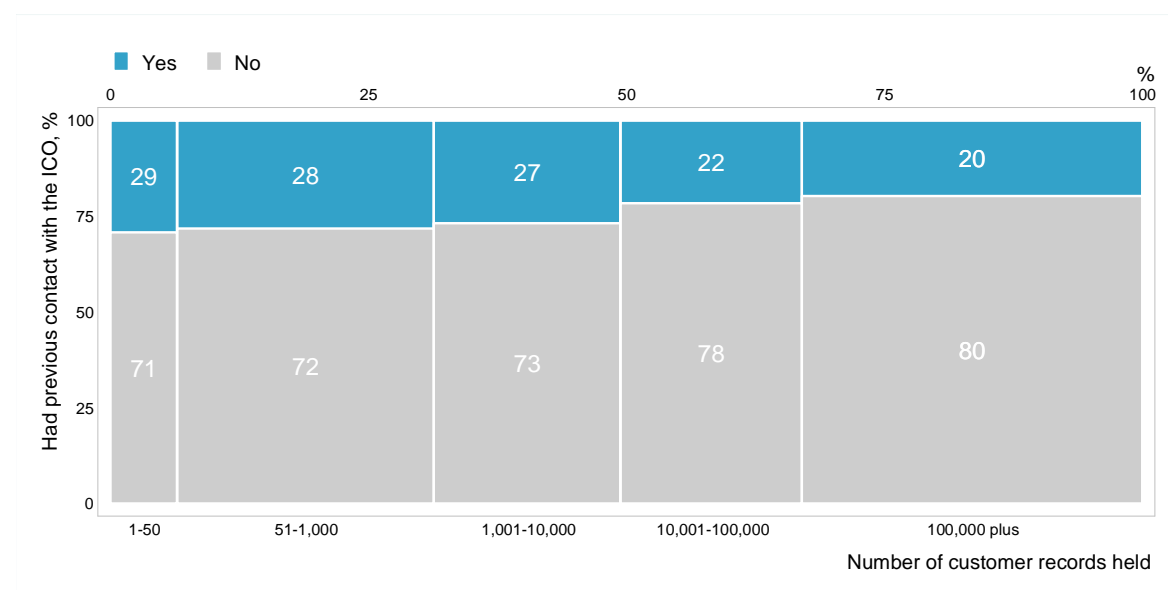
- A fairly small proportion of firms in our sample have been in contact with the ICO (at most 30% for different levels of data intensity and 21% overall);
- Companies that are smaller and handle relatively fewer records of personal data are more likely to have had contact with the ICO in the past⁵⁶; and,
- Companies who had previous contacts with the ICO are much more likely to approach the ICO concerning the new Regulation.

⁵⁴ See footnote 1 above.

⁵⁵ Note that our sample does not provide enough observations to make meaningful comparisons across individual sectors (SIC); see the breakdown of the sample by sector in Table 6, Annex A1.3.1.

⁵⁶ Note that this may also reflect the fact that smaller companies are likely to have less in-house expertise. In addition, the ICO may spend a lot of time on a single contact with large company and small amounts of time on multiple contacts with smaller ones.

Figure 22: Likelihood of having prior contact with the ICO given the number of customer records



Source: London Economics

Table 5: Likelihood of approaching the ICO in the future

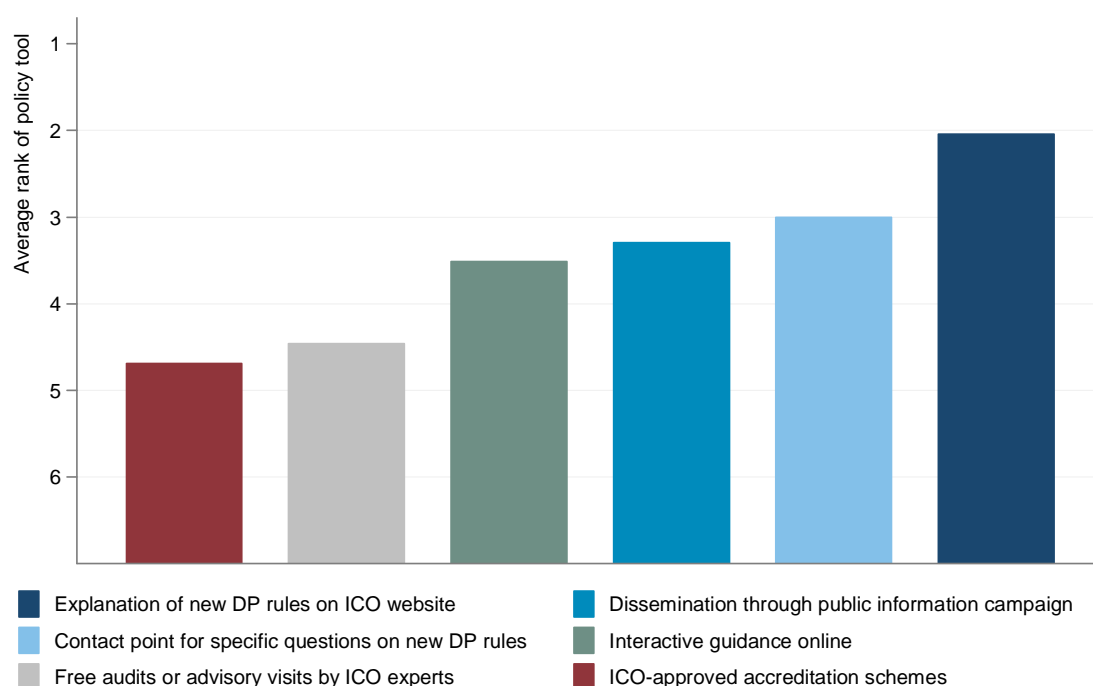
Had previous contact with the ICO	Will approach the ICO in the future		Total
	Unlikely (%)	Likely (%)	
No	76.4	23.7	241
Yes	28.8	71.3	80
Total	64.5	35.5	321

Source: London Economics

4.2 Practical support and guidance the ICO could provide to businesses

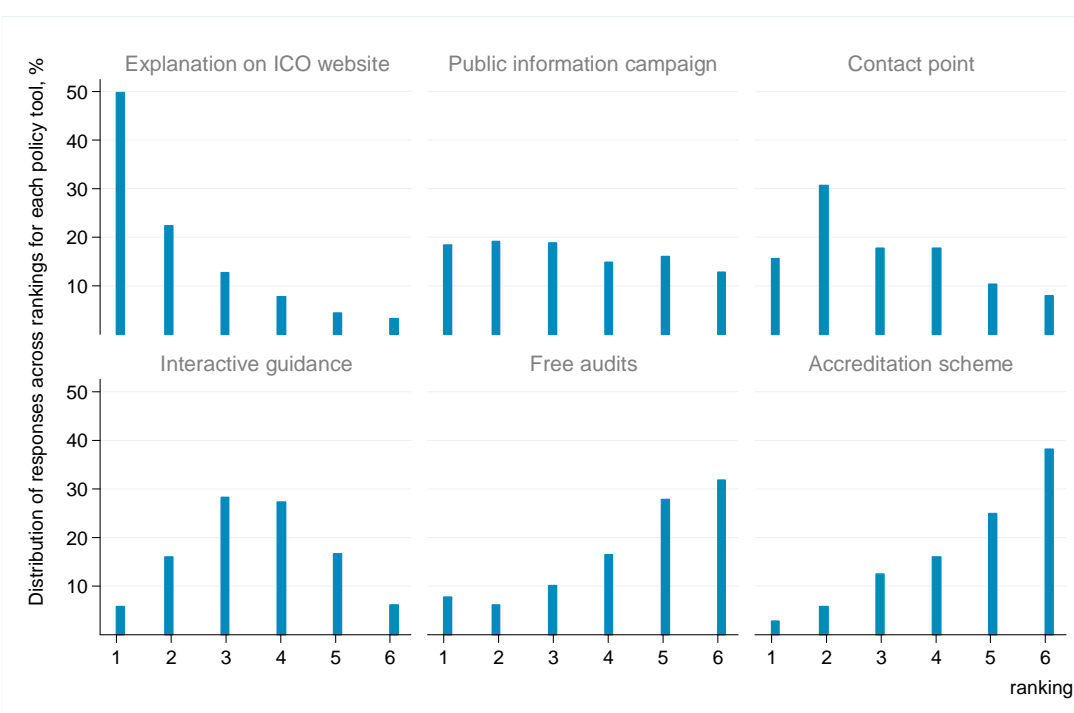
Companies were asked to rank different types of support that the ICO may offer to assist in the transition to the new data protection Regulation. Provision of clear and concise guidance about the scope of the new provisions (changes from the status quo) available on the ICO's website is unambiguously the form of ICO support that is seen as most beneficial. Second to this is a contact point (phone hotline, email, live chat, etc.) to deal with specific questions regarding the new data protection rules. On the other hand, ICO approved accreditation or certification schemes on specific areas of compliance are seen as the least beneficial in relation to the transition to the new Regulation. However, average ranks for all options are positive, which suggests that each form of support might have a role, either on its own or in combination with others, in providing effective assistance to businesses. The issue of support options, including the interaction between different types of engagement, warrants further investigation.

Figure 23: Average ranking per support option



Source: London Economics

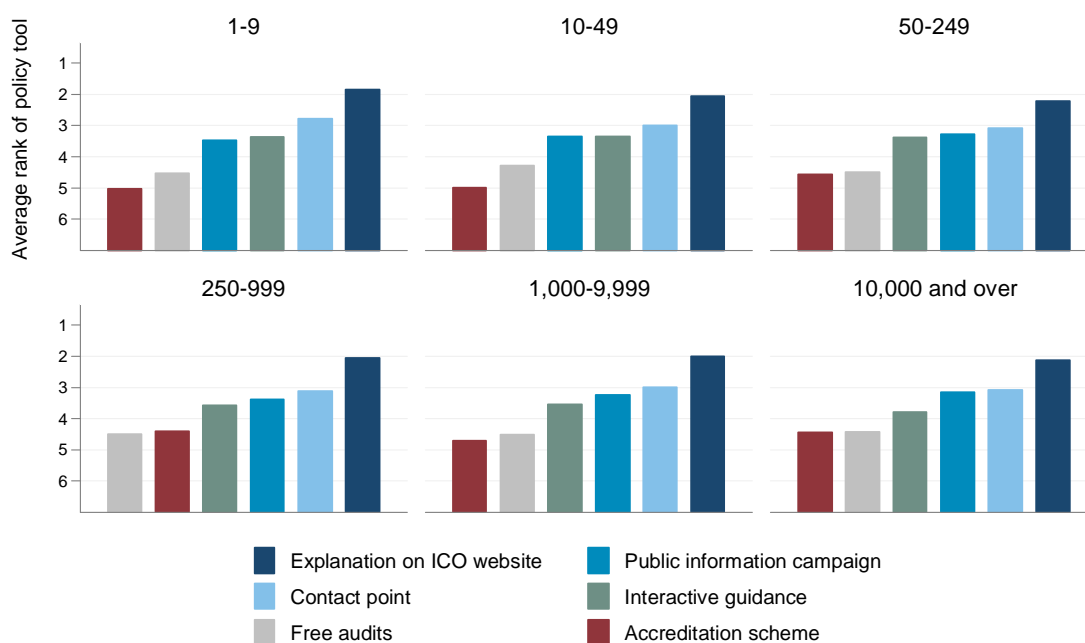
Figure 24: Distribution of rankings for each support option



Source: London Economics

These key findings are very robust and are confirmed by analysis by firm size (number of employees, Figure 25 below), sector⁵⁷, data intensity⁵⁸, knowledge of the provisions⁵⁹ and previous contact with the ICO⁶⁰. Public information campaigns are seen to be slightly more useful on average by larger companies (50+ employees) and do not rank significantly lower than an ICO contact point. Interactive guidance is seen slightly more positively by businesses in the service sector (“other services”), which may reflect the fact that certain engagement channels are more effective with specific types of businesses.

Figure 25: Average ranking of support options by firm size



Graphs by Number of employees

Source: London Economics

Overall, the analysis suggests that the ICO should focus its business support activities on making information available and accessible through various channels (both on the website and through a manned contact point). A parallel information campaign should be used alongside measures to provide information to businesses on demand.

In terms of a potential focus on individual sectors, the ICO’s priorities should naturally include those sectors which store and use significant amounts of personal information, or data of a particularly sensitive nature, notably financial services, public administration, health, online

⁵⁷ Figure 32, A1.3.4.

⁵⁸ Figure 33, A1.3.4.

⁵⁹ Figure 28, A1.3.4.

⁶⁰ Figure 29, A1.3.4.

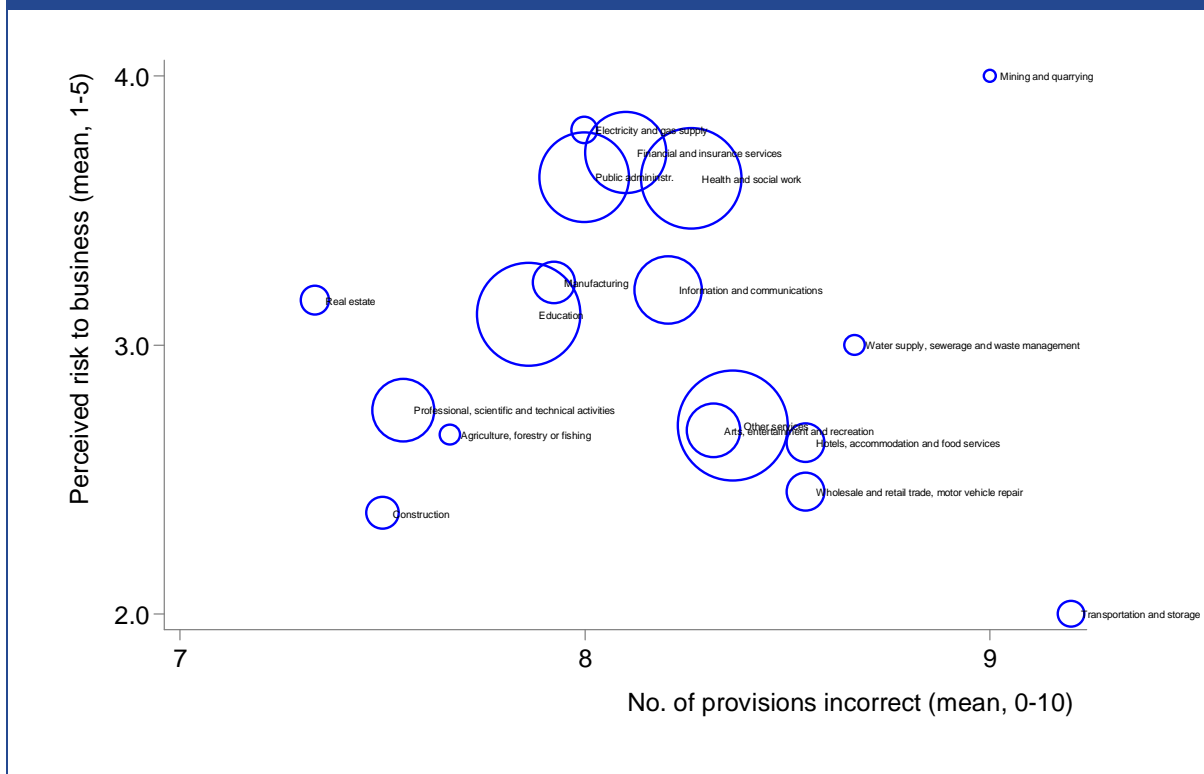
services and marketing. Naturally, businesses holding more information face potentially greater risks, and should therefore be prioritised by the ICO.⁶¹

Our survey provides some evidence as to the sectors in which ICO support is needed most, either because they face particular risks from breaches of data protection or because knowledge of the proposed Regulation is low (Figure 26). In the former category, our survey confirms that organisations in health and social work, financial and insurance services and public administration warrant the ICO's attention. These sectors combine high perceived risk with relatively low levels of knowledge about the proposed Regulation. Knowledge also is limited in the services sector, even though risks are seen as lower. Low sample sizes in individual sectors (small circles in Figure 26) prevent us from analysing this issue in greater detail.

In practical terms Figure 6 above (p. 25) showed that even seemingly straightforward measures like the provisions on fines and DPO requirements are insufficiently understood by many businesses. Therefore, while the ICO should focus on those measures that have been identified as the most burdensome by business, there is no reason for the ICO to limit its focus further or concentrate on specific measures.

⁶¹ There often is a positive association between the number of records of personal data held by a company and its size. In our survey sample, the correlation coefficient between categorical measures of no. of records held and no. of employees is > 0.4). However, the correspondence is imperfect; in the digital economy, small businesses (e.g. in online services) may hold and process vast amounts of personal information (for example, in our sample, 10% of the companies in the "other services" sector with less than 50 employees report holding more than 100,000 data records on their customers or third-party individuals).

Figure 26: Knowledge gaps and business risk by sector



Note: the size of the circles is proportional to the number of survey responses (e.g., 3 respondents in sector “agriculture, forestry or fishing”; 90 responses in sector “other services”).

Source: London Economics

4.3 Summary

Box 6: Key findings

- A lack of understanding about the provisions in the EC’s proposed general data protection Regulation persists across business. Uncertainty is pervasive across the provisions of the proposed regulation, and affects more abstract and unsettled aspects, such as the obligations of data controllers under the so-called right to be forgotten, as well as seemingly straightforward changes such as those regarding administrative fines and the appointment of Data Protection Officers.
- The majority of businesses are unable to quantify their current spending in relation to data protection responsibilities under existing law – and this persists in relation to estimates for expected future spending under the new proposals. This uncertainty indicates that existing evidence on the financial impact of the regulation are difficult to corroborate. Further research is required to clarify some important issues, such as the role of privacy and data protection in determining the level and intensity of consumer participation in online markets.
- The lack of understanding that the research reveals strongly indicates that there is a key role for the ICO to play in educating and supporting businesses to increase their awareness and understanding of the forthcoming changes. The ICO’s priorities for supporting business in implementing the new Regulation should focus on providing guidance on the areas of the new provisions which are shown to be misunderstood – for example the ‘right to be forgotten, but also the new rules on fines, the appointment of Data Protection Officers, Subject Access

Requests and data portability.

- While uncertainty affects all industries, the ICO should focus its liaison work on organisations involved in data-intensive activities, who face economic risks from breaches of data protection rules, and who are active in sectors where knowledge of the rules seems to be particularly low. The study finds evidence that the service sector in general, and specifically health, finance and insurance and public administration⁶² should be prioritised.

On 25 January 2012, The European Commission published new legislative proposals for data protection, with the aim of enhancing online privacy rights of individuals and reducing legal fragmentation in the EU. The idea behind the proposed Regulation is to increase consumer confidence in the online channel, and at the same time facilitate the free flow of information within the European Union, so as to “foster economic growth, innovation and job creation”.

Reactions to the proposal are mixed. Stakeholders welcome its contribution towards updating EU data protection law to reflect the digitalisation of how information is gathered, stored and shared. However, there are concerns that the proposal puts too much emphasis on demonstrating compliance, and too little on achieving results. Feedback from stakeholders in the UK suggests that the benefits from increased consumer protection, improved access to data and enhanced control of its use may be offset by the costs of implementation and compliance to business. These costs may be so high as to put European businesses at a competitive disadvantage, globally.

In its Impact Assessment, the European Commission estimated an overall net benefit of £2 billion arising from the reduced administrative burden of complying with a unified EU law, rather than a multiplicity of national rules. The MoJ’s call for Evidence, on the other hand, shows a variety of different appraisals from stakeholders in the UK that report much higher costs of compliance than those laid out by the EC. The MoJ’s own Impact Assessment expects the Regulation to cost UK businesses alone somewhere between £80 and £320 million per year.

We find that considerable uncertainty surrounds these cost estimates. This is based on very strong evidence from a unique new survey of individuals with data protection responsibilities in UK companies. In particular, the survey demonstrates widespread and pervasive uncertainty about actual data protection costs, as well as the content and implications of the proposed reforms to the European data protection framework.

What emerges from the survey is that 82% of firms (that are, to varying degrees, affected by data protection concerns) are unable to quantify how much they currently spend on data protection; and 87% are unable to quantify the expected additional impact of the new Regulation. This lack of knowledge of the cost of data protection, even by individuals whose job entails data protection responsibilities, along with the apparent lack of awareness or understanding of the most sensitive provisions, casts doubts on some of the more extreme cost estimates voiced by stakeholders. Moreover, the highly skewed distributions of both current and future expected spending on data protection suggest that many of these figures are applicable to only a very small minority of UK companies.

⁶² See footnote 1 above.

Based on evidence from stakeholders, provisions that are likely to have the most significant impact on UK businesses include (i) the higher standard for obtaining consent from data subjects; (ii) the strengthened rights of data subjects to access their personal data, transfer it to other organisations, and demand its removal of from third party records; (iii) the stricter obligations of data controllers to provide information to individuals, notify breaches of security to authorities and actively demonstrate compliance with the Regulation; and (iv) the punitive administrative sanctions that authorities are required to impose in the event of non-compliance with the Regulation.

However, in a number of instances, our survey analysis reveals evidence of a positive correlation between lack of knowledge of the provisions and its expected additional cost to business. This correlation appears to reflect, on the one hand, an overly onerous perception of certain provisions on the part of firms, and on the other, a general sense of complexity and lack of clarity in the provisions themselves.

Business activities that are likely to be negatively affected by these new provisions involve direct marketing, e-commerce and digital advertising, particularly in relation to the new consent requirements. However, the ICT sector is also expected to be affected by reductions in investment and limitations on the ability to develop new digital media applications. This outcome is particularly costly both to business and to society as it constrains innovation and dynamism in an industry that contributes heavily to large-scale economic growth.

Despite the notable costs that many sources have reported in relation to the abovementioned provisions, there are also some key benefits to business, particularly from imposing stricter obligations on controllers. In fact, more stringent checks on how data controllers make use of personal information, combined with a shift in the burden of proof of compliance, will likely reduce negligent misuse of data and as result reduce the occurrence of personal data breaches. The MoJ estimates that this will save UK businesses £58 to £124 million per year on the whole. This may also serve to attain the EC's primary goal of enhancing consumer confidence in the digital market, which will indirectly also benefit business. The same caveats as above regarding the reliability of these estimates apply, given the uncertainty about the scope and impact of the Regulation.

Finally, the Regulation is expected to achieve (to some extent) the Commission's other key objective – reducing legal fragmentation in the EU. Based on the Commission's Impact Assessment, the MoJ estimate that this will reduce administrative burdens born by UK businesses somewhere in the range of £42 million to £66 million⁶³.

Based on the findings of uncertainty associated with even qualitative cost estimates in the London Economics survey, we consider the existing evidence on the net impact of the proposed Regulation as weak. More research is needed to clarify a number of important issues, not least the role of privacy and data protection in determining the level and intensity of consumer participations in online markets.

⁶³ However, Kuner (2012) warns that “the commendable reduction of bureaucracy in some areas is at least partially offset by the introduction of other procedural requirements”.

In the meantime, we are on firmer ground with our recommendations on the ICO's role in supporting businesses in the phase of transition to the new European data protection framework.

Provision by the ICO of clear and concise guidance about the scope of the new provisions (changes from the status quo) available on the ICO's website is unambiguously the form of ICO support that is seen as most beneficial by respondents to our survey, followed by more intensive support through an interactive a contact point (phone hotline, email, live chat, etc) to deal with specific questions regarding the new data protection rules.

In contrast, ICO-approved accreditation or certification schemes on specific areas of compliance are seen as the least beneficial. These findings are robust along a number of dimensions, including business size, data-intensity and previous contact with the ICO.

However, note that these findings too have to be judged in the context of uncertainty about the scope of the provisions. It is possible that greater clarity will increase the demand for certification schemes, for example, while the preference for pure information provision we find among respondents might itself be evidence of the prevailing lack of clarity. This does not affect the implications for the ICO's business engagement strategy in the near term, which itself has to operate in an environment of incomplete information about the eventual shape of the Regulation. The evidence suggests that the ICO should make information available and accessible through various channels (both on the website and through a manned contact point). The ICO should focus on raising businesses' awareness of the future ICO guidance and advice that will be available (both on the website and through its helpline). This could take the form of an active information campaign. Finally, the ICO should ensure that it reaches the organisations that suffer most from a combination of lack of knowledge of data protection rules and risk from data protection breaches. Examples of possible priority areas include health and social work, financial and insurance services, public administration⁶⁴, as well as businesses in the broader services sector.

⁶⁴ See footnote 1 above.

References

Acquisti, A., Brandimarte, L. And Loewenstein, G. (2010), 'Misplaced Confidences: Privacy and the Control Paradox', *Ninth annual workshop on the economics of information security (WEIS)*.

Acquisti, A., Friedman, A. and Telang, R. (2006), 'Is there a cost to privacy breaches? An event study', *Workshop on the Economics of Information Security (WEIS)*, University of Cambridge, UK.

Bartlett, J. (2012), 'The Data Dialogue', published by Demos.

Billmonitor (2012), *The billmonitor.com national mobile phone report 2012* (June).

Department for Business, Innovation & Skills (2012), 'Midata 2012 review and consultation'. Available at: <http://bit.ly/XyCi7l> [Accessed 5 February 2013].

Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003), 'The economic cost of publicly announced information security breaches: Empirical evidence from the stock market', *Journal of Computer Security*, 11, 3, 431–448.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2002), 'The effect of internet security breach announcements on market value of breached firms and internet security developers', in *International Journal of Electronic Commerce*, 9.

Chatterjee, D. Richardson, V. J. and Zmud, R. W. (2001), 'Examining the Shareholder Wealth Effects of Announcements of Newly Created CIO Positions', *MIS Quarterly*, 25, 1, 43-70.

Davidson III, W. L. and Worrell, D. L. (1992), "The Effect of Product Recall Announcements on Shareholder Wealth", *Strategic Management Journal*, 13, 6, 467-473.

DMA (2012), *Putting a price on direct marketing 2012*.

Dos Santos, B. L., Peffers, K. and Mauer, D. (1993), 'The Impact of Information Technology on the Market Value of the Firm', *Information Systems Research* (March): 1-23.

European Commission (1995), Directive 95/46/EC of 24 October 1995 on the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Commission (2012), 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', COM (2012) 11 final.

European Commission (2012), 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', COM (2012) 10 final.

European Commission (2012), Staff working Paper Executive Summary of the Impact Assessment, SEC (2012) 73 final.

FutureSight (2011), 'User perspectives on mobile privacy', *Summary of research findings*, a presentation prepared for GSMA, September 2011.

Garrick, T. (2012), 'DMA reveals potential costs of EU Data Protection Regulation to business', 15 March. Available at: <http://bit.ly/wFkUPQ> [Accessed 5 February 2013].

Graux, H., Ausloos, J. and Valcke, P. (2012), 'The Right to be Forgotten in the Internet Era', *ICRI Working Paper Series* (October): p.16.

Hovava, A. and D'Arcy, J. (2003), 'The impact of denial-of-service attack announcements of the market value of firms', *Risk Management and Insurance Review*, 6, 2, 97–121.

Hendricks, K. and Singhal, V. (1997), 'Delays in new product introductions and the market value of the firm: The consequences of being late to the market', *Management Science*, 43, 4, 422–436.

Im, K. S., Dow, K. E. and Grover, V. (2001), 'Research Report: A Reexamination of IT Investment and the Market Value of the Firm – An Event Study Methodology', *Information Systems Research*, 12, 1, 103–117.

Information Commissioner's Office (2012), 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework', 27 February.

Infosecurity, PwC (2012), *Information Security Breaches Survey 2012, Technical report*. Available at: <http://pwc.to/KcUncl> [Accessed 5 February 2013]

Internet Advertising Bureau (2012), 'Written Evidence from IAB UK', *House of Commons Justice Select Committee Inquiry into EU Data Protection Framework Proposals*. Available at: <http://bit.ly/Y60MOa> [Accessed 5 February 2013].

Jarrell, G. and Peltzman, S. (1985), 'The Impact of Product Recalls on the Wealth of Sellers', *The Journal of Political Economy*, 93, 3, 512–536.

Kuner, C. (2012). "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law". *Bloomberg BNA Privacy and Security Law Report*, Vol. 6. Available at: <http://ssrn.com/abstract=2162781> [accessed 16 April 2013].

Le Merle et al. (2012), 'The impact of US internet privacy regulations on early-stage investments. A quantitative study', Booz&Co.

London Economics (2010), 'Study on the Economic Benefits of Privacy-enhancing Technologies (PETs)'. Report to EC DG Justice. Available at: <http://bit.ly/12U6cLR> [accessed 28 April 2013].

Ministry of Justice (2012), 'Call for Evidence on Proposed EU Data Protection Legislative Framework', Summary of Responses, 28 June.

Ministry of Justice (2012), 'Proposal for an EU Data Protection Regulation Impact Assessment', 22 November.

Office of Information Commissioner (2005), *Annual Report 2004*. Available at: <http://bit.ly/12JNW7I> [Accessed 5 February 2013].

Frontier Economics (2006), 'Independent review of the impact of the Freedom of Information Act', A Report prepared for the Department for Constitutional Affairs (October).

Reding, V. (2012), 'Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for business', Speech presented at the European Commission press release, 25 January 2012. Available at: <http://bit.ly/14aCxAl> [Accessed 5 February 2013].

Rosen, J. (2012), 'The Right to Be Forgotten', 64 *Stan. L. Rev. Online* 88, 13 February. Available at: <http://bit.ly/x1gkNJ> [Accessed 5 February 2013].

Telang, R. and Wattal, S. (2006), 'Impact of software vulnerability announcements on the market value of software vendors - An empirical investigation', Working Paper, Carnegie Mellon University.

Tucker, C. (2011): "Social networks, personalized advertising, and perceptions of privacy control", NET Institute Working Paper No. 10-07; MIT Sloan Research Paper No. 4851-10. <http://bit.ly/iT1ATt> (accessed 17 September 2012).

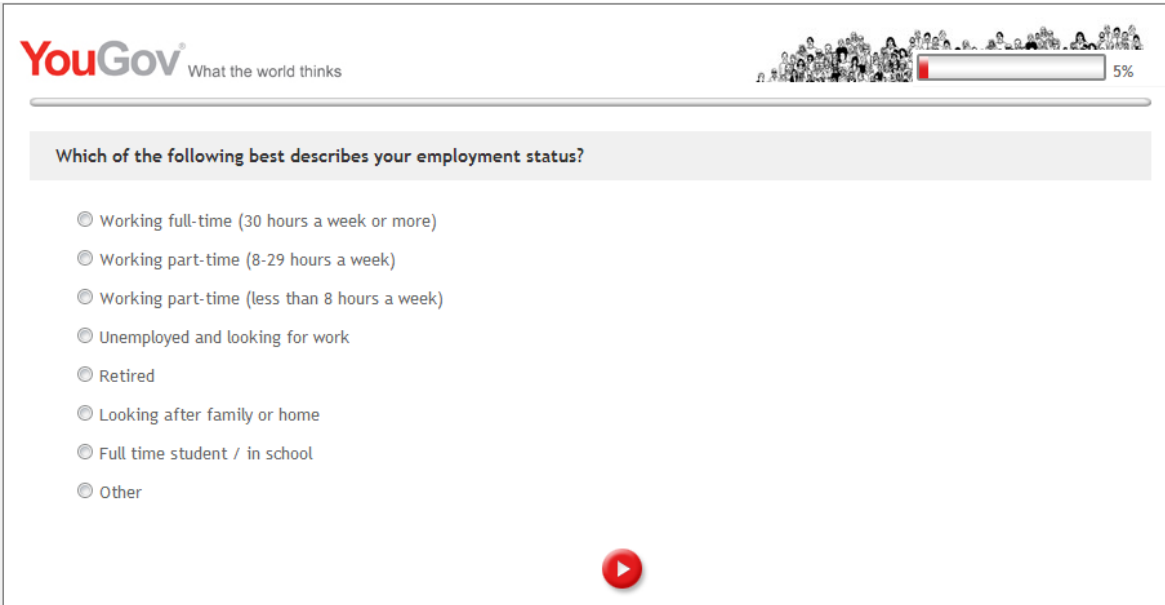
VeriSign (2009), 'One in Eight Brits Fall Victim to Online ID Fraud', Press Release about YouGov survey, 16 September 2009. Available at: <http://bit.ly/11T6gaB> [Accessed 5 February 2013].

Annex 1 Survey of businesses



A1.1 Sampling

The sampling process began with a screening exercise to identify people with responsibility for data protection issues where they worked. In a regular screening survey of the entire YouGov panel of 400,000 UK adults we asked those in full or part time employment to pick out their areas of responsibility. Data protection was one of 11 areas of responsibility listed; others included office supplies, marketing, IT support, customer services, finance, etc. This generated a pool of around 1,700 people with responsibility for data protection. The final screening criterion was to exclude the self-employed or single person business through a question about the number of employees working for their organisation. Invitations to participate were issued at random using the pool of 1,700 until 506 responses were received.

A1.2 The questionnaire






The screenshot shows a YouGov survey interface. At the top left is the YouGov logo with the tagline 'What the world thinks'. At the top right is a progress bar showing 5% completion. The main question is 'Which of the following best describes your employment status?'. Below the question are eight radio button options: 'Working full-time (30 hours a week or more)', 'Working part-time (8-29 hours a week)', 'Working part-time (less than 8 hours a week)', 'Unemployed and looking for work', 'Retired', 'Looking after family or home', 'Full time student / in school', and 'Other'. A red play button is centered at the bottom of the question area.


What the world thinks


How many employees work in your organisation?

- ☐ Just me
- ☐ 1-9
- ☐ 10-49
- ☐ 50-249
- ☐ 250-999
- ☐ 1,000-9,999
- ☐ 10,000 and over





What the world thinks




In a recent survey you indicated that you have responsibility for Data Protection issues where you work..

This survey is about how data protection affects organisations in terms of the handling of the personal details of customers, suppliers or employees for example.


Please indicate if you are able to answer questions about data protection.


- ☐ Yes I can answer questions about Data Protection
- ☐ No, I can't answer questions about Data Protection




What the world thinks


Welcome to this survey which is about data protection issues. Please answer based on your role and responsibilities for data protection where you work. Your YouGov account will be credited with 50 points for completing the survey. We have tested the survey and found that, on average it takes around 10 minutes to complete. This time may vary depending on factors such as your internet connection speed and the answers you give.



YouGov What the world thinks 

In which of these sectors does your business or organisation primarily operate?

In how many EU countries (excluding the UK) does your company regularly operate?

☐ Don't Know

Does your organisation have a member of staff with a job role focused on data protection compliance, for example a data protection officer?


☐ Yes


☐ No

☐ Not sure

How many staff in your company have roles related to data protection and information security?

☐ Don't Know





YouGov What the world thinks 

In the question below, by 'personal information' we mean any information that can be linked to a specific individual with reasonable accuracy, that is, any data that is referenced with an individual's name, address, telephone number, email etc.

Please specify which personal information (e.g. contact details, salaries, past purchases, etc.) your company keeps ...


	None	Contact details only	Contact details and other information	Don't know
Customers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Suppliers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Third-parties (e.g. commercial marketing databases)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>




YouGov What the world thinks  35%

Can you estimate how many records are kept?


	None	1-50	51-1,000	1,001-10,000	10,001-100,000	100,000 plus	Don't know
Customers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Suppliers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Third-parties (e.g. commercial marketing databases)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>





YouGov What the world thinks  40%

On what scale, if any, does your organisation derive economic benefits from holding personal information of the following types? This might be through increased sales through more targeted marketing, better management of supplier relationships etc.

	1 - No Benefits	2	3	4	5 - Very large benefits
Customers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Staff	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Suppliers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Third-parties (e.g. commercial marketing databases)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



 What the world thinks



Breaches of data security or customer's and business partners' concerns about data protection could harm your business (e.g. legal claims, official fines or other sanctions, loss of trust). How do you judge the risk for your business?

☐ 1 - No risk

☐ 2

☐ 3

☐ 4

☐ 5 - Great risk

Does your company regularly transfer personal data outside the UK?


☐ Yes, within the EU



☐ Yes, outside the EU

☐ Yes, both within and outside the EU

☐ No

☐ Not sure




What the world thinks


The European Commission has proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. The Commission's proposals update and modernise the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights in the future.

We now have a set of questions about different aspects of the reforms.

Definition of personal data

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ IP addresses and cookie identifiers always constitute personal data
- ☐ The definition of personal data makes no mention of online identifiers, cookies or IP addresses
- ☐ If online identifiers provided by an individual's device leave traces that combined with other information can be used to identify the person in question, this constitutes personal data
- ☐ Not sure

Consent requirements

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ Personal data may only be processed if the data subject has given explicit consent to having their personal data processed
- ☐ When personal data is being collected online, users must not be able to use the service for which their personal data is being collected while their consent is verified
- ☐ Personal data may be processed if the data subject has not explicitly opted out of the processing of their personal data
- ☐ Not sure

Data minimisation


Please select the statement that best describes the new rules proposed by the European Commission


- ☐ Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- ☐ The data controller is required to agree upon the maximum time for which personal data can be kept before collecting or processing any personal data
- ☐ Personal data must be limited to the minimum necessary in relation to the purposes for which they are processed
- ☐ Not sure

Please estimate how costly you expect these to be to implement in your business?

	1 - No additional costs	2	3	4	5 - Substantial additional costs	Not sure / not applicable
Definition of personal data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Consent requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data minimisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>




What the world thinks


58%

Subject Access Requests

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ The data subject has the right to obtain from the controller access to his or her data without constraint at reasonable intervals and without excessive delay or expense
- ☐ The data subject has the right to obtain from the controller access to his or her data free of charge under all circumstances
- ☐ That data subject has the right to obtain from the controller access to his or her data free of charge, unless the data controller can prove that such requests are manifestly excessive
- ☐ Not sure

Right to be forgotten

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ If the data subject requests erasure of personal data relating to him or her, the controller must ensure that all links to, or copies and replications of such personal data be erased
- ☐ A controller that has made personal data public must inform third parties of the data subject's request to erase any links to, or copy or replication of that personal data
- ☐ If the data subject requests rectification or erasure of his or her personal data, the controller must notify any third parties to whom this data was disclosed of this request, unless disproportionately costly
- ☐ Not sure

Data portability

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ The data subject has the right to obtain his or her personal data in a commonly used format and transfer it to other organisations
- ☐ The data controller must provide access to the data subject's personal data, but the Regulation makes no mention of which format this data must be presented in
- ☐ Upon request, the data controller must issue a copy of a subject's personal data in a format mandated by the European Commission
- ☐ Not sure

Please estimate how costly you expect these to be to implement in your business?

	1 - No additional costs	2	3	4	5 - Substantial additional costs	Not sure / not applicable
Subject Access Requests	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Right to be forgotten	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data portability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Data protection officer

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ Companies with 250+ employees or whose core activities involve the processing of personal must appoint (an existing or new employee) as data protection officer
- ☐ All companies with 250+ employees or whose core activities involve data processing must hire a new employee to cover the role of data protection officer
- ☐ Companies that appoint a data protection officer are not required to notify the supervisory authority of their data processing activities
- ☐ Not sure

Breach notification

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ There is no obligation on controllers to report breaches of security that result in loss, release or corruption of personal data
- ☐ All personal data breaches must be notified to all interested parties without undue delay
- ☐ All personal data breaches must be notified to the supervisory authority within 24 hours
- ☐ Not sure

Administrative fines

Please select the statement that best describe the new rules proposed by the European Commission

- ☐ A fine of 2% of annual turnover must be applied in all instances of infringement of the Regulation
- ☐ The ICO must impose a fine of up to 2% of a firm's global annual turnover for the most serious breaches of the Regulation
- ☐ The ICO can issue a penalty of up to £500,000 for the most serious breaches of the Regulation
- ☐ Not sure

Data protection impact assessments


Please select the statement that best describe the new rules proposed by the European Commission

- ☐ Data controllers are required to notify supervisory authorities of their processing activities and provide a general description of the measures taken to ensure data security
- ☐ Data controllers are required to carry out a data protection impact assessment prior to processing operations that present specific risks to the rights of data subjects
- ☐ Data controllers are required to carry out a data protection impact assessment prior to any processing operations
- ☐ Not sure

Please estimate how costly you expect these to be to implement in your business?

	1 - No additional costs	2	3	4	5 - Substantial additional costs	Not sure / not applicable
Data protection officer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Breach notification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Administrative fines	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data protection impact assessments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



YouGov What the world thinks 

Please can you estimate how much (£) your organisation currently spends on data protection and information security per year? Please type in

☐ Don't Know

Have concerns about complying with data protection law prevented you from developing new business activities or processes?

☐ Yes

☐ No

☐ Don't know / not sure

How much (£) do you expect to spend additionally as a one-off cost to comply with the new data protection rules?

☐ Don't Know

How much (£) do you expect to spend additionally each year to comply with the new data protection rules?


☐ Don't Know


Do you expect the proposed new data protection rules to prevent you from developing new business activities?

☐ Yes

☐ No

☐ Don't know / not sure




YouGov What the world thinks 


Have you had any previous contact(s) with the Information Commissioner's Office (ICO)?

☐ Yes

☐ No


☐ Not sure




YouGov What the world thinks  73%

How likely would you be to approach the ICO for assistance with implementing the new data protection rules?

☐ Likely
☐ Unlikely
☐ Not sure



YouGov What the world thinks  78%

What type of assistance by the ICO would you regard as beneficial? Please rank in order of importance with 1 being the most important and 6 the least important.

Drag your choices onto the numbered boxes on the right to rank each of the characteristics below.

Provision of clear and concise guidance about the scope of the new provisions (changes from the status quo) available on the ICO's website

Active dissemination of clear and concise information about the scope of the new provisions (changes from the status quo) through public information campaign (mail shots, posters, broadcasts, etc.)

Contact point (phone hotline, email, live-chat etc.) to deal with specific questions regarding the new data protection rules

Provision of interactive guidance such as online training, seminars, toolkits, customisable materials

Free audits or advisory visits by ICO experts

ICO approved accreditation / certification schemes on specific areas of compliance.

RANKINGS

1


2

3


4

5

6



YouGov[®] What the world thinks


 82%

To date have you received guidance on data protection rules from a trade association or industry body for your sector?


☐ Yes

☐ No

☐ Not sure



YouGov[®] What the world thinks


 87%

Would you be interested in receiving such guidance from a trade association or industry body for your sector?

☐ Yes

☐ No

☐ Don't know



A1.3 Summary statistics of survey respondents

A1.3.1 Business demography

Table 6: Sectoral distribution of survey participants

Sector of activity	Frequency	%
Agriculture, forestry or fishing	3	0.59
Mining and quarrying	1	0.2
Manufacturing	13	2.57
Electricity and gas supply	5	0.99
Water supply, sewerage and waste management	3	0.59
Construction	8	1.58
Wholesale and retail trade, motor vehicles	11	2.17
Transportation and storage	5	0.99
Hotels, accommodation and food services	11	2.17
Information and communications	34	6.72
Financial and insurance services	49	9.68
Real estate	6	1.19
Professional, scientific and technical	29	5.73
Public administration and defence	61	12.06
Education	79	15.61
Health and social work	76	15.02
Arts, entertainment and recreation	22	4.35
Other services	90	17.79
Total	506	100

Source: London Economics

A1.3.2 Characteristics of firms that employ staff with data protection responsibilities

Table 7: Size of firms that employ staff with data protection responsibilities

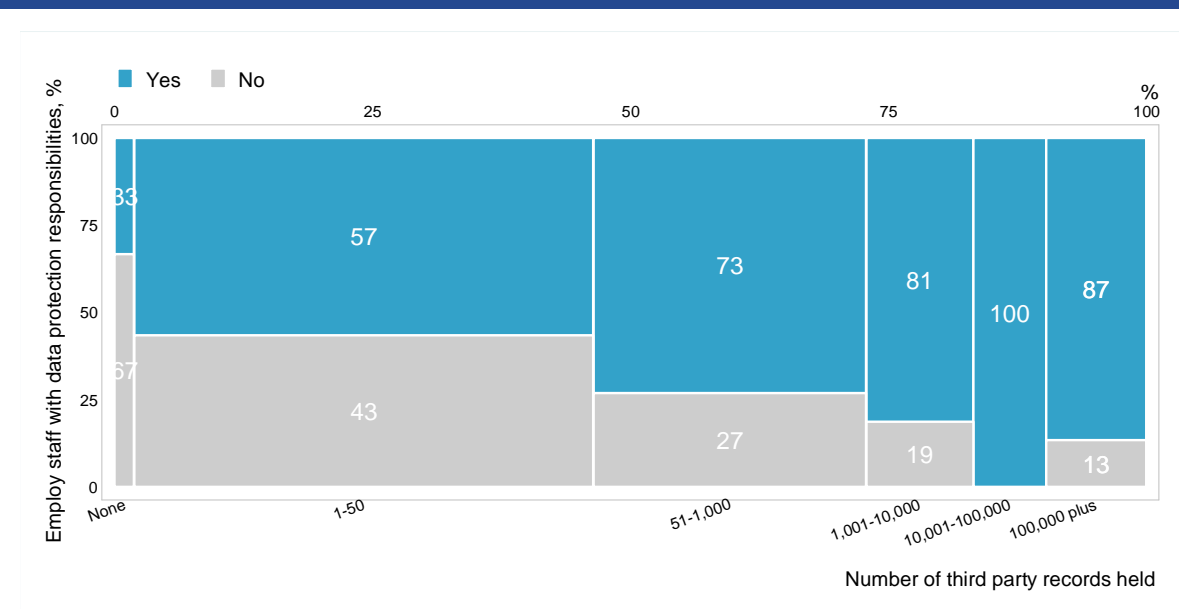
Number of employees	Employs staff with DP responsibilities		
	No (%)	Yes (%)	Total
1-9	74.67	25.33	75
10-49	70.83	29.17	72
50-249	49.06	50.94	53
250-999	24.07	75.93	54
1,000-9,999	2.65	97.35	113
10,000 and over	3.61	96.39	83
Total	33.78	66.22	450

Source: London Economics

Table 8: Data intensity of firms that employ staff with data protection responsibilities: number of customer records

Number of <i>customer</i> records	Employs staff with DP responsibilities		
	No (%)	Yes (%)	Total
1-50	45.83	54.17	24
51-1,000	70.00	30.00	90
1,001-10,000	46.77	53.23	62
10,001-100,000	27.42	72.58	62
100,000 plus	6.09	93.91	115
Total	35.98	64.02	353

Source: London Economics

Figure 27: Likelihood of employing staff with data protection responsibilities given number of third party records

Source: London Economics

Table 9: Data intensity of firms that employ staff with data protection responsibilities: number of third party records

Number of <i>third party</i> records	Employs staff with DP responsibilities		
	No (%)	Yes (%)	Total
None	66.67	33.33	3
1-50	43.48	56.52	69
51-1,000	26.83	73.17	41
1,001-10,000	18.75	81.25	16
10,001-100,000	0.00	100.00	11
100,000 plus	13.33	86.67	15
Total	30.97	69.03	155

Source: London Economics

Table 10: Risk of harm to business from data security concerns by firms that employ staff with data protection responsibilities

Risk to business	Employs staff with DP responsibilities		
	No (%)	Yes (%)	Total
1 - No risk	59.18	40.82	49
2	55.26	44.74	114
3	26.55	73.45	113
4	25.97	74.03	77
5 - Great risk	10.31	89.69	97
Total	33.78	66.22	450

Source: London Economics

Table 11: Expected additional cost of provision on DPOs by firms that employ staff with data protection responsibilities

Expected additional cost of DPO provision	Employs staff with DP responsibilities		
	No (%)	Yes (%)	Total
1 - No additional cost	37.5	62.5	104
2	16.67	83.33	30
3	26.42	73.58	53
4	31.82	68.18	22
5 - Substantial additional cost	39.39	60.61	33
Not sure	35.58	64.42	208
Total	33.78	66.22	450

Source: London Economics

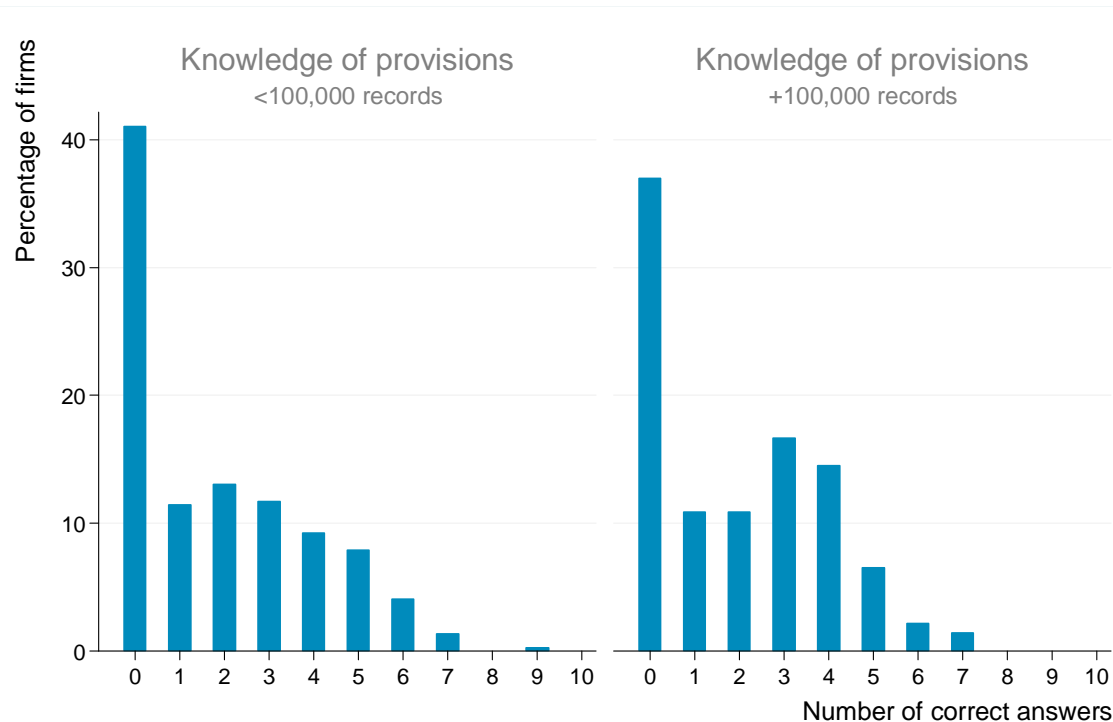
Table 12: Restrictions on the development of new business activities or processes

		Employs staff with DP responsibilities	
		No (%)	Yes (%)
Current Regulation	No	39.49	60.51
	Yes	25.00	75.00
New Regulation	No	35.61	64.39
	Yes	33.33	66.67

Source: London Economics

A1.3.3 Knowledge of provisions

Figure 28: Knowledge of provisions by volume of data (on customers and third parties) held by companies



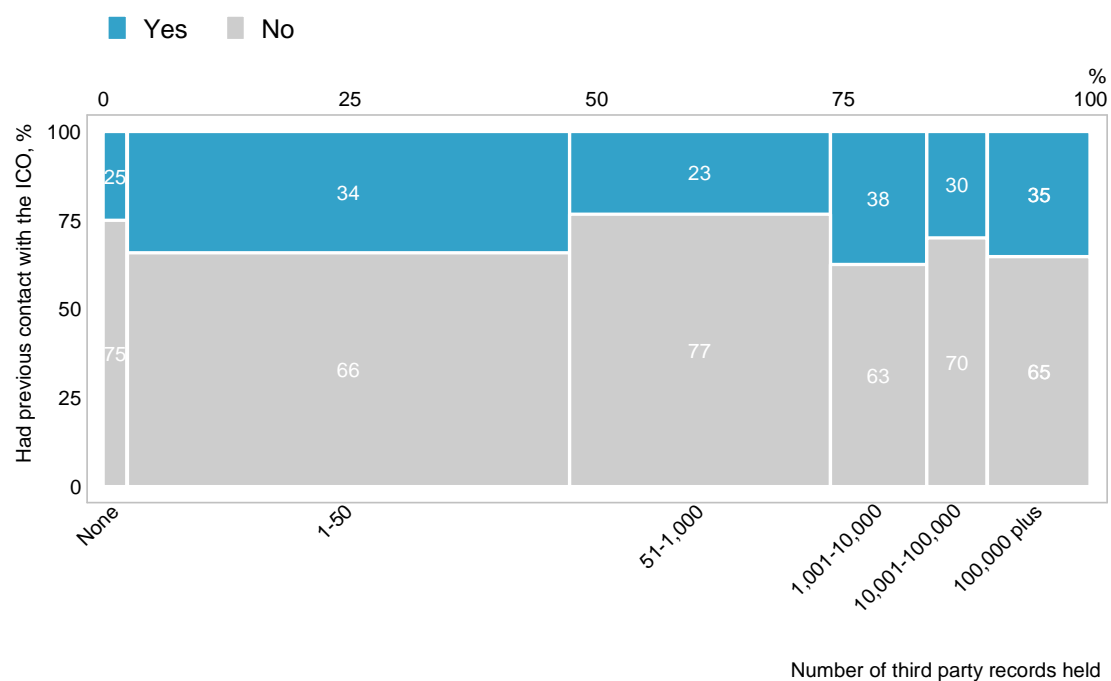
Source: London Economics

A1.3.4 ICO assistance

Table 13: Data intensity of firms that had previous contact with the ICO: number of customer records

Number of customer records	Had previous contact with the ICO		
	No (%)	Yes (%)	Total
1-50	70.83	29.17	24
51-1,000	71.74	28.26	92
1,001-10,000	73.13	26.87	67
10,001-100,000	78.46	21.54	65
100,000 plus	80.33	19.67	122
Total	75.95	24.05	370

Source: London Economics

Figure 29: Likelihood of having prior contact with the ICO given the number of third party records

Source: London Economics

Table 14: Data intensity of firms that had previous contact with the ICO: number of third party records

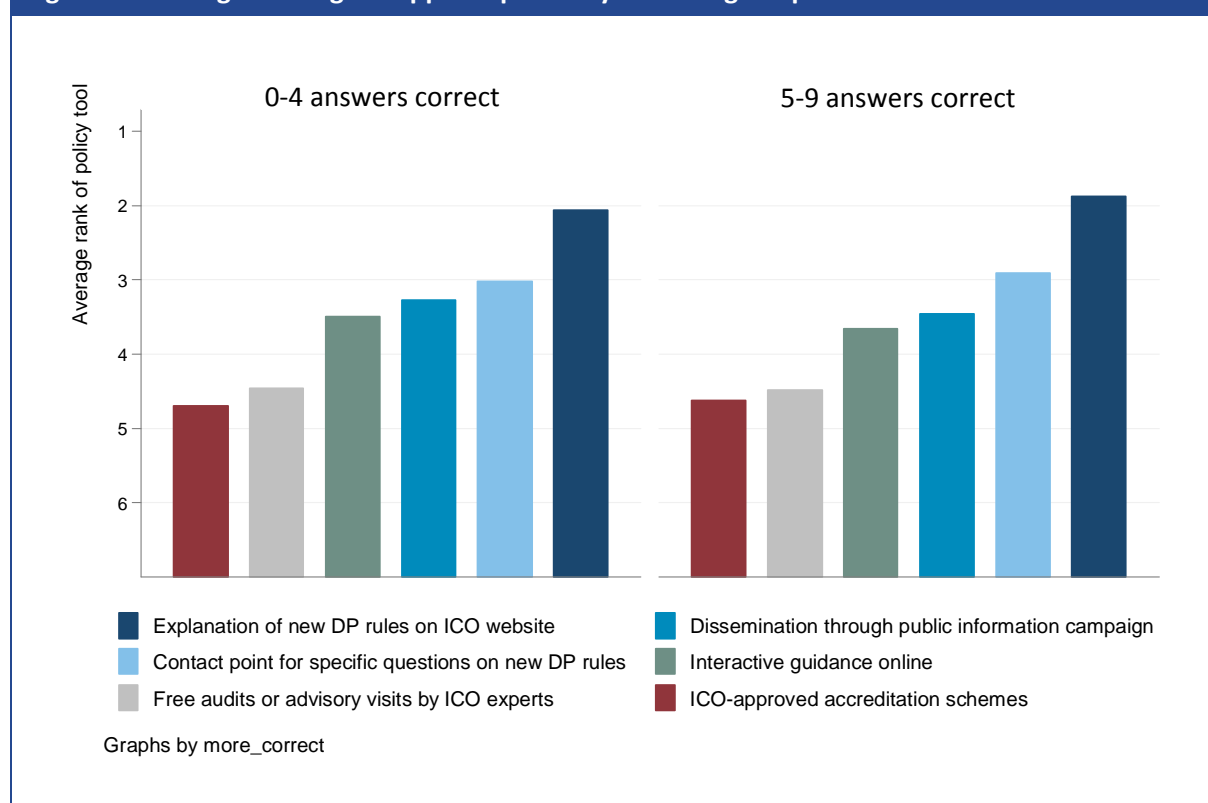
Number of third party records	Had previous contact with the ICO		Total
	No (%)	Yes (%)	
None	75	25	4
1-50	65.75	34.25	73
51-1,000	76.74	23.26	43
1,001-10,000	62.5	37.5	16
10,001-100,000	70.00	30.00	10
100,000 plus	64.71	35.29	17
Total	68.71	31.29	163

Source: London Economics

Table 15: Frequency of ranking score for policy tools available to the ICO

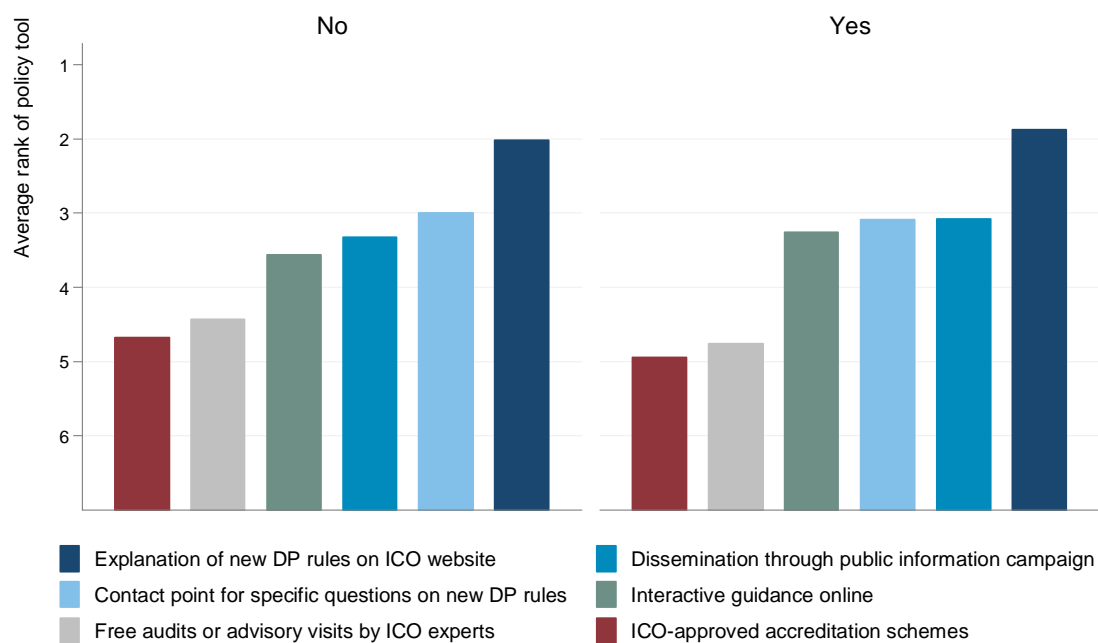
Policy tool	1 st	2 nd	3 rd	4 th	5 th	6 th
Explanation of new DP rules on ICO website	252	113	64	39	22	16
Dissemination through public information campaign	93	97	95	75	81	65
Contact point for specific questions on new DP rules	79	155	90	90	52	40
Interactive guidance online	29	81	143	138	84	31
Free audits or advisory visits by ICO experts	39	31	51	83	141	161
ICO-approved accreditation schemes	14	29	63	81	126	193

Source: London Economics

Figure 30: Average ranking of support options by knowledge of provisions

Source: London Economics

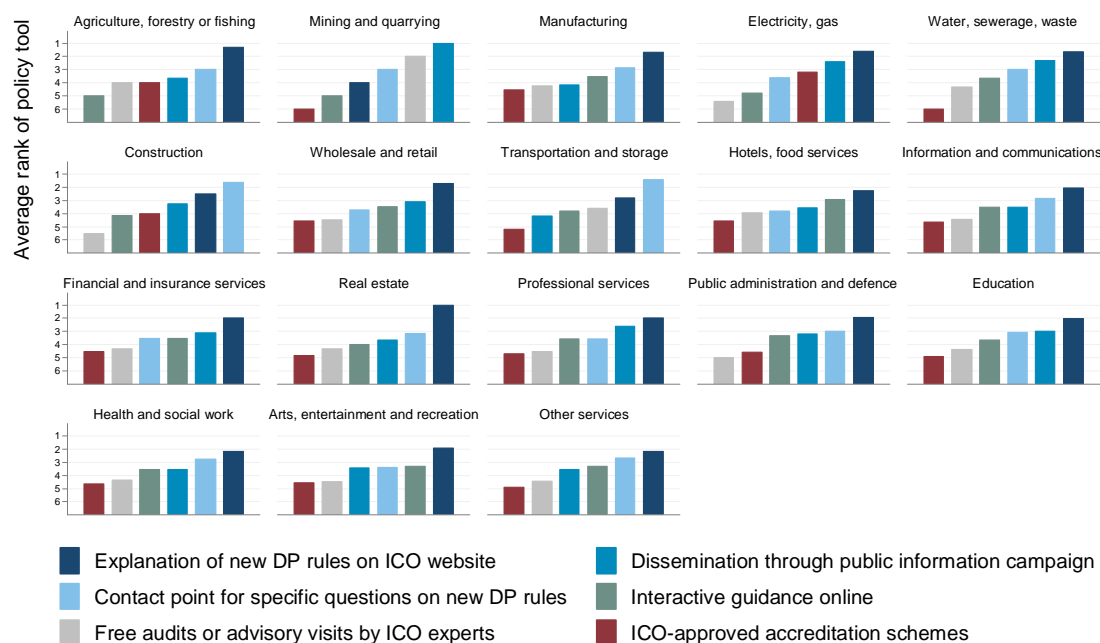
Figure 31: Average ranking of support options by previous contact with the ICO



Graphs by Has had previous contact with the ICO

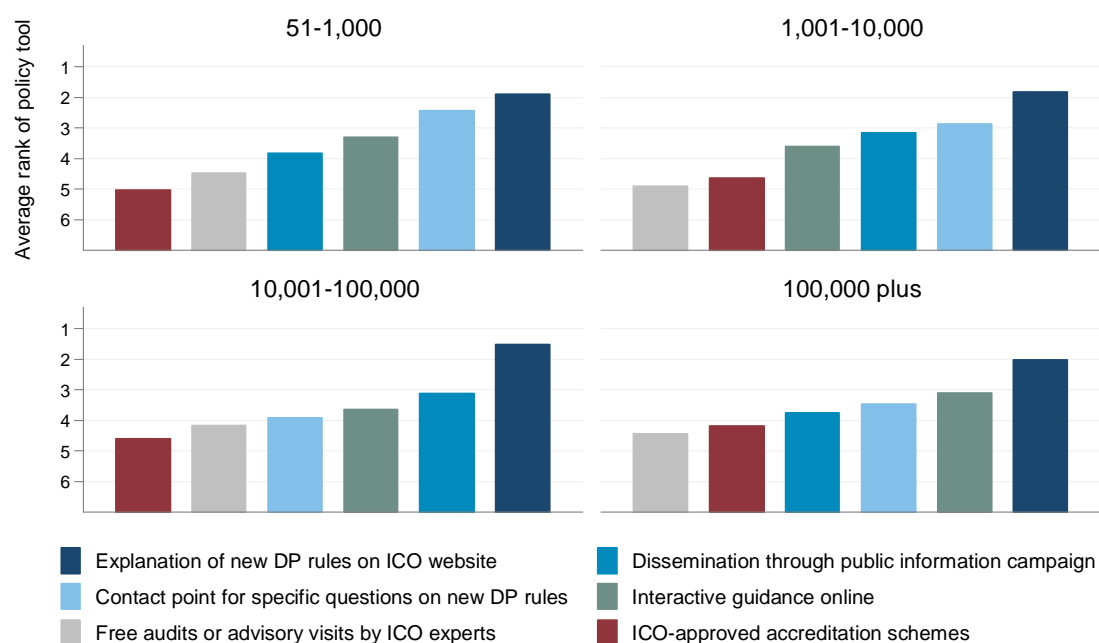
Source: London Economics

Figure 32: Average ranking of support options by sector



Source: London Economics

Figure 33: Average ranking of support options by data intensity (no. of records held)



Note: no. of records is the highest of no. of records on customers and no. of record on 3rd parties.

Source: London Economics

A1.4 Econometric analysis

A1.4.1 Regression for overall costs

Table 16: Regression output: expected additional cost of new Regulation
(1= no additional costs; 5 = substantial additional costs)

Explanatory factors	cost
derives large benefit from holding personal data	0.565*** (0.201)
knowledge of provisions	0.143 (0.322)
(derives large benefit from holding personal data)*(knowledge of provisions)	-0.355* (0.188)
Staff with DP responsibilities	0.280 (0.220)
(Staff with DP responsibilities)*(knowledge of provisions)	0.0727 (0.264)
Risk of harm to business	0.219*** (0.0757)
(Risk of harm to business)*(knowledge of provisions)	0.125 (0.362)
Constant	1.554*** (0.238)
Observations	294
R-squared	0.177

Standard errors in parentheses

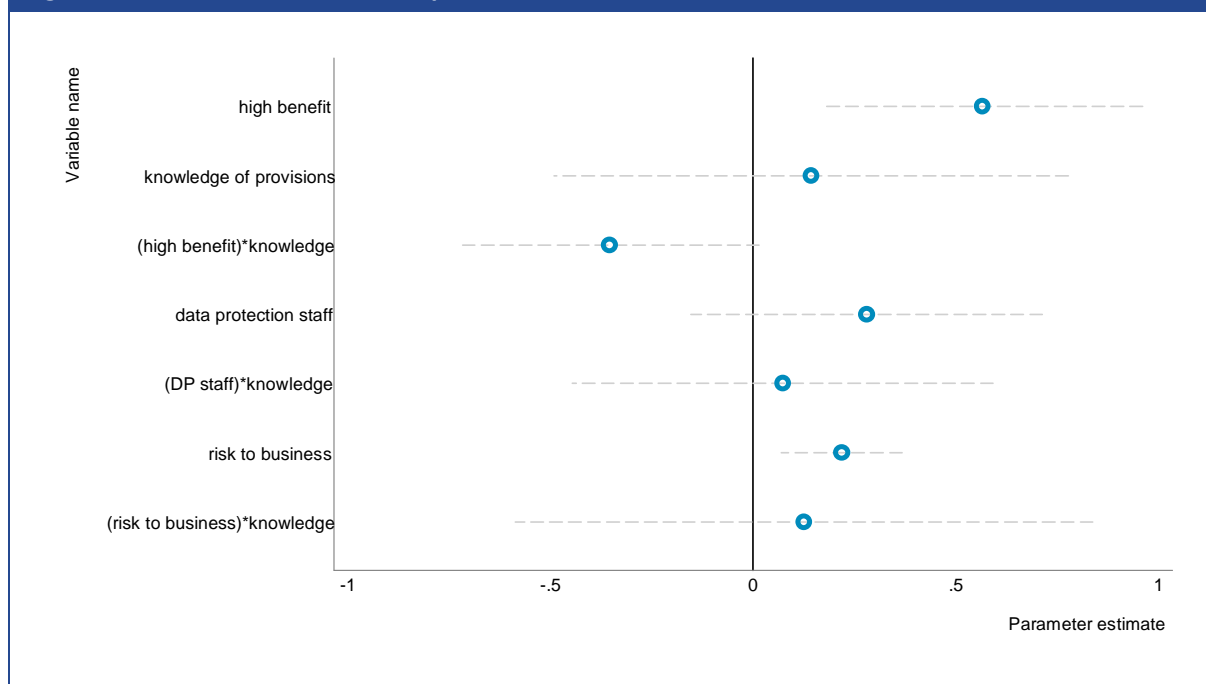
*** p<0.01, ** p<0.05, * p<0.1

**Table 17: Regression output: expected additional cost of new Regulation
(1= no additional costs; 5 = substantial additional costs)**

Explanatory factors	cost
derives large benefit from holding personal data	0.459** (0.197)
knowledge of provisions	0.195 (0.304)
(derives large benefit from holding personal data)*(knowledge of provisions)	-0.385** (0.182)
Risk of harm to business	0.193*** (0.0685)
(Risk of harm to business)*(knowledge of provisions)	0.170 (0.338)
Regular transfer of personal data within the EU	0.265** (0.113)
Regular transfer of personal data outside the EU	0.302*** (0.0978)
Regular cross-border transfer of personal data (EU & extra-EU)	0.185 (0.119)
Constant	1.717*** (0.222)
Observations	289
R-squared	0.175

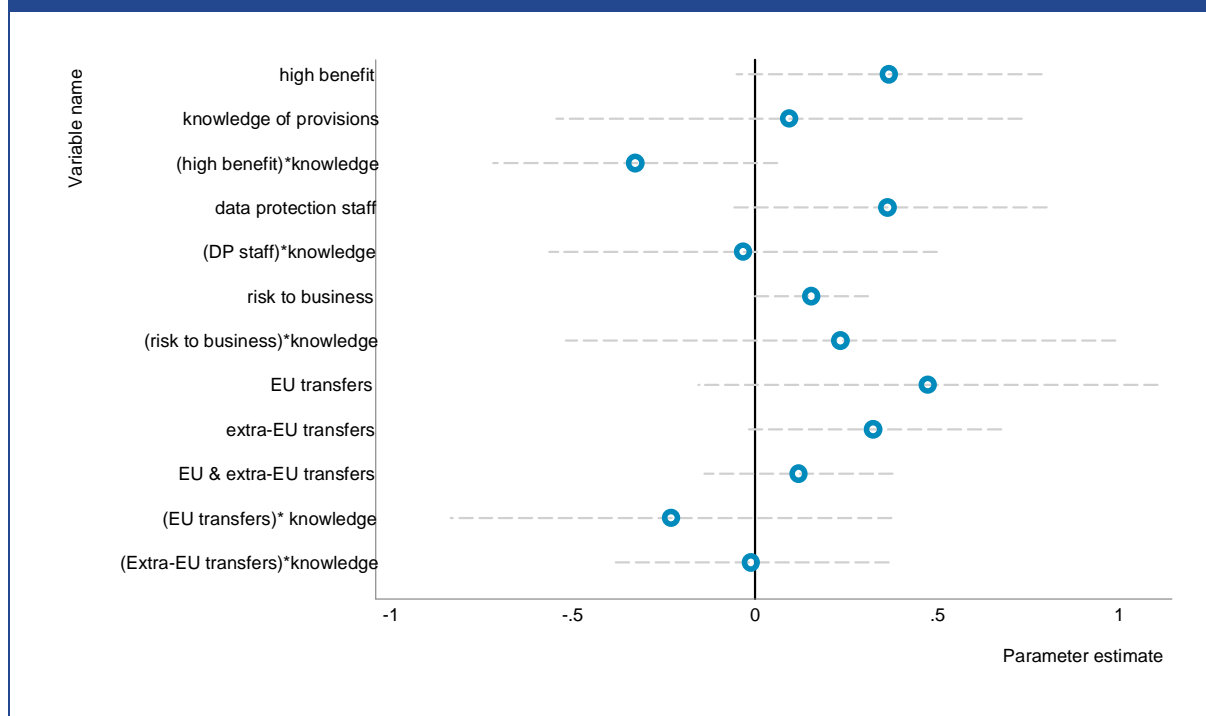
Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Figure 34: Predictors of overall expected additional cost

Note: All input variables used in this estimation are standardised so as to make the parameter estimates comparable across variables.

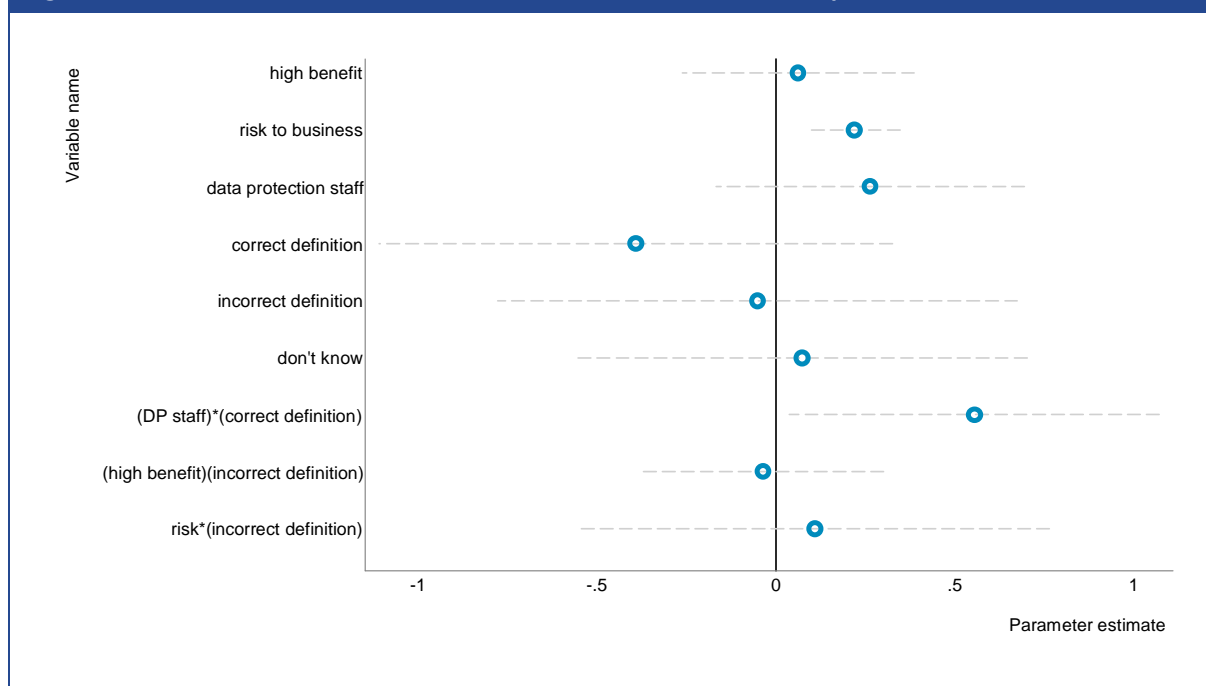
Source: London Economics

Figure 35: Predictors of overall expected additional cost of Regulation, accounting for regular cross-border transfer of data

Source: London Economics

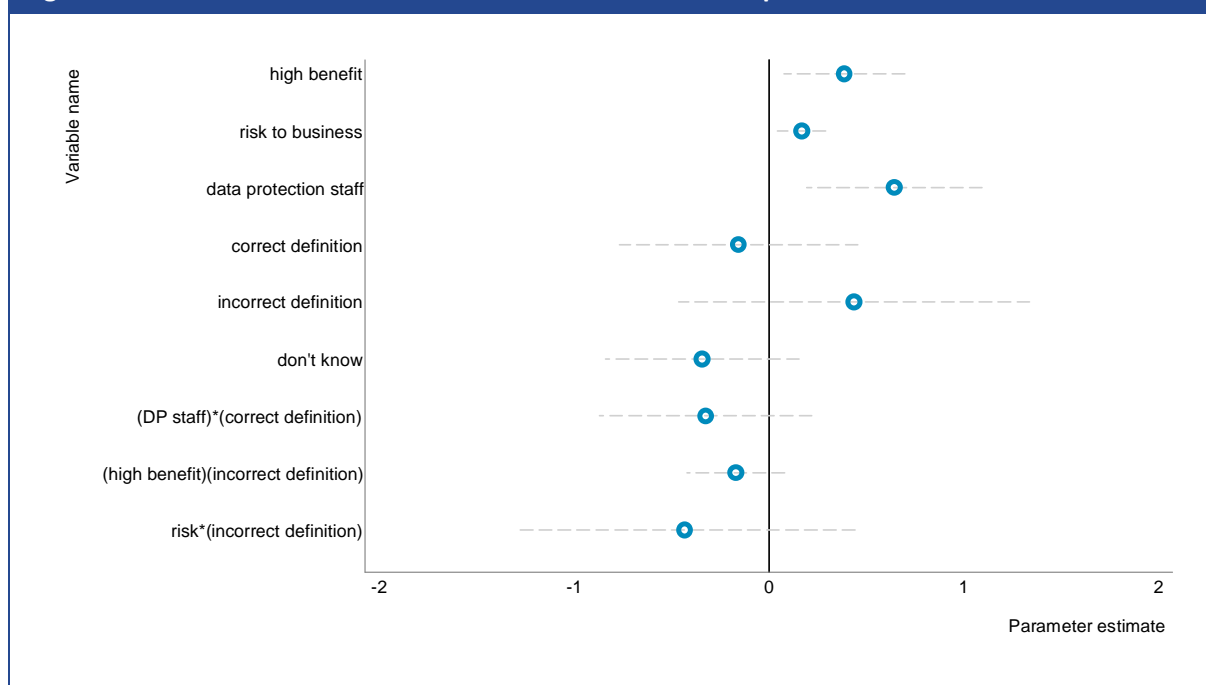
A1.4.2 Cost regressions by provision

Figure 36: Predictors of additional cost related to the definition of personal data



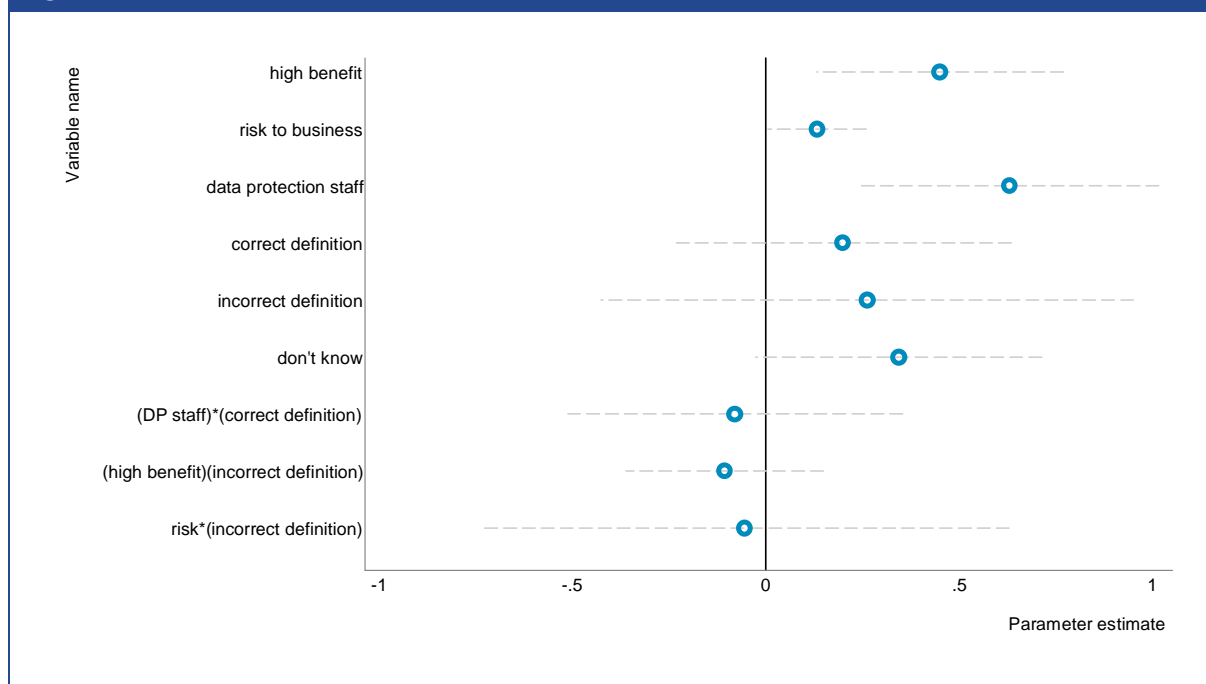
Source: London Economics

Figure 37: Predictors of additional cost related to consent requirements



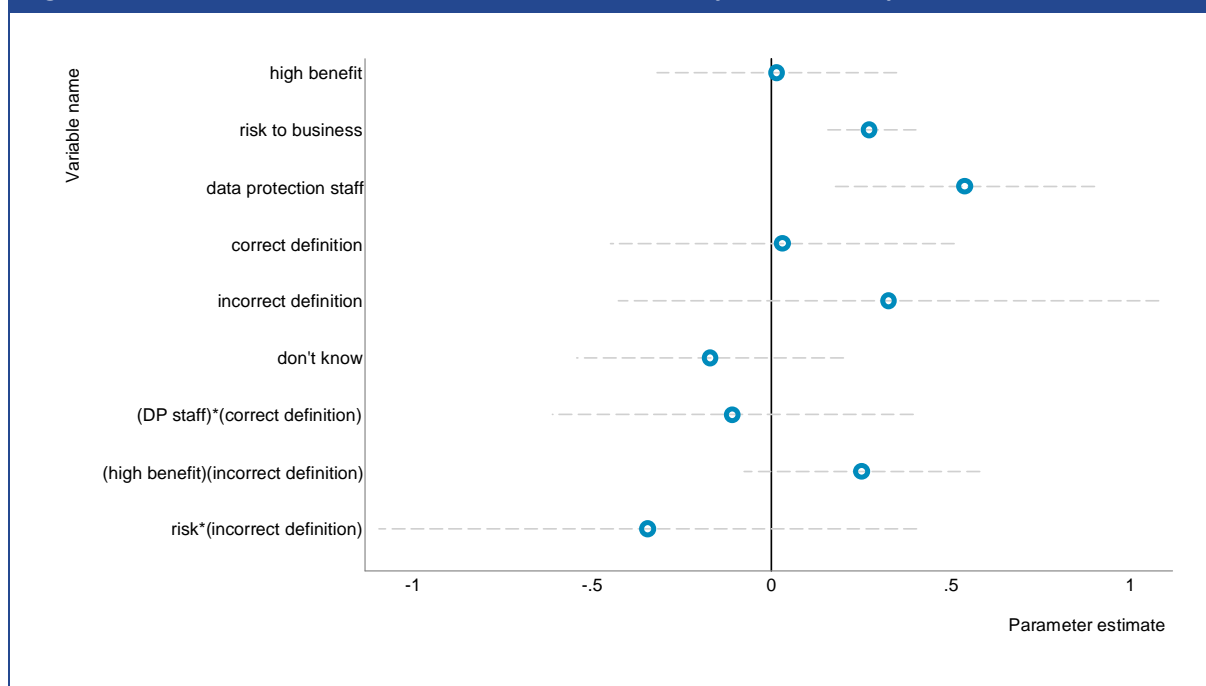
Source: London Economics

Figure 38: Predictors of additional cost related to data minimisation



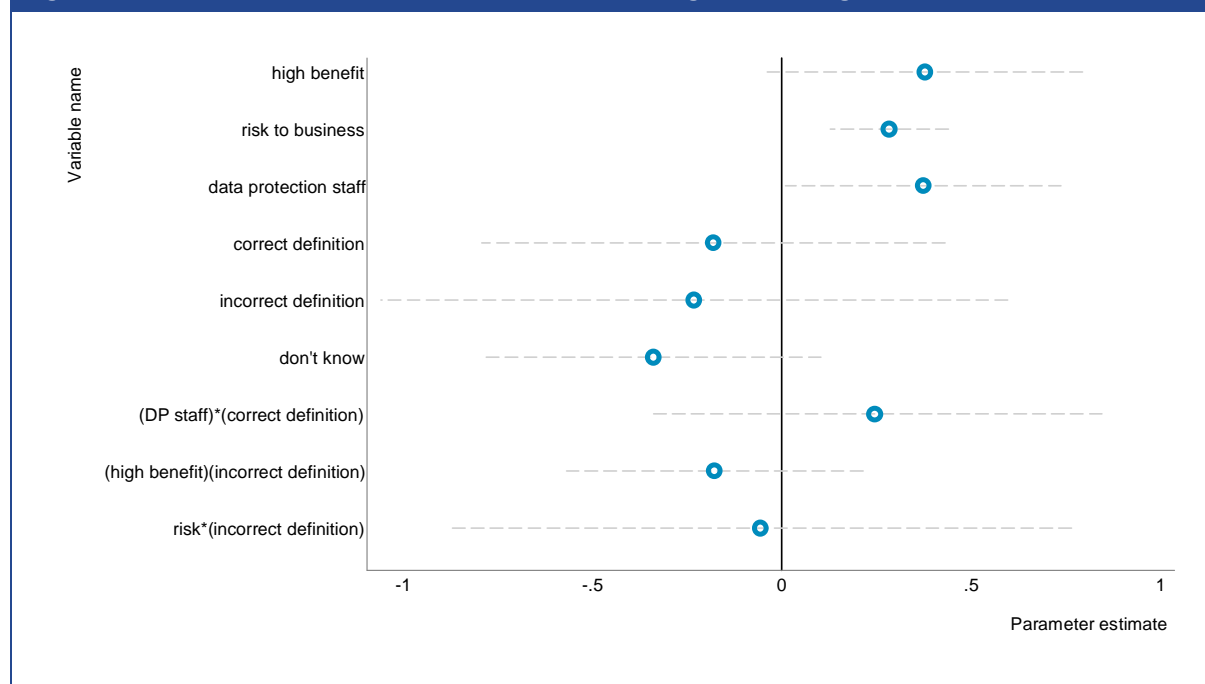
Source: London Economics

Figure 39: Predictors of additional cost related to the subject access requests



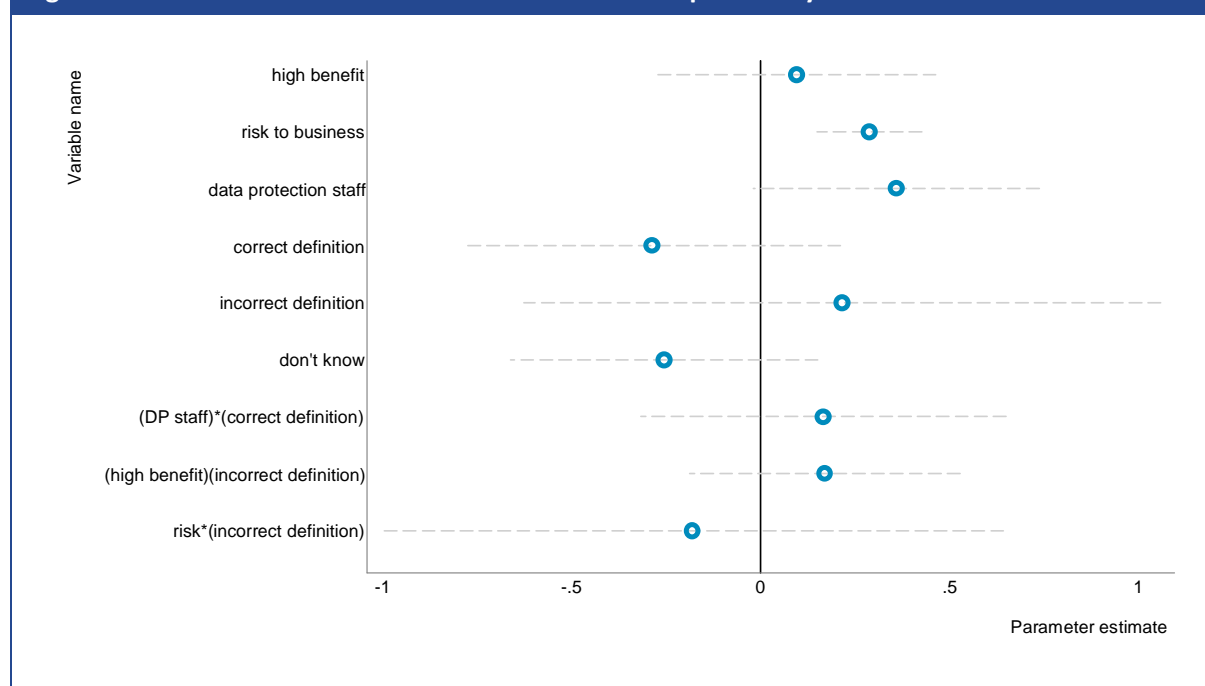
Source: London Economics

Figure 40: Predictors of additional cost related to the right to be forgotten

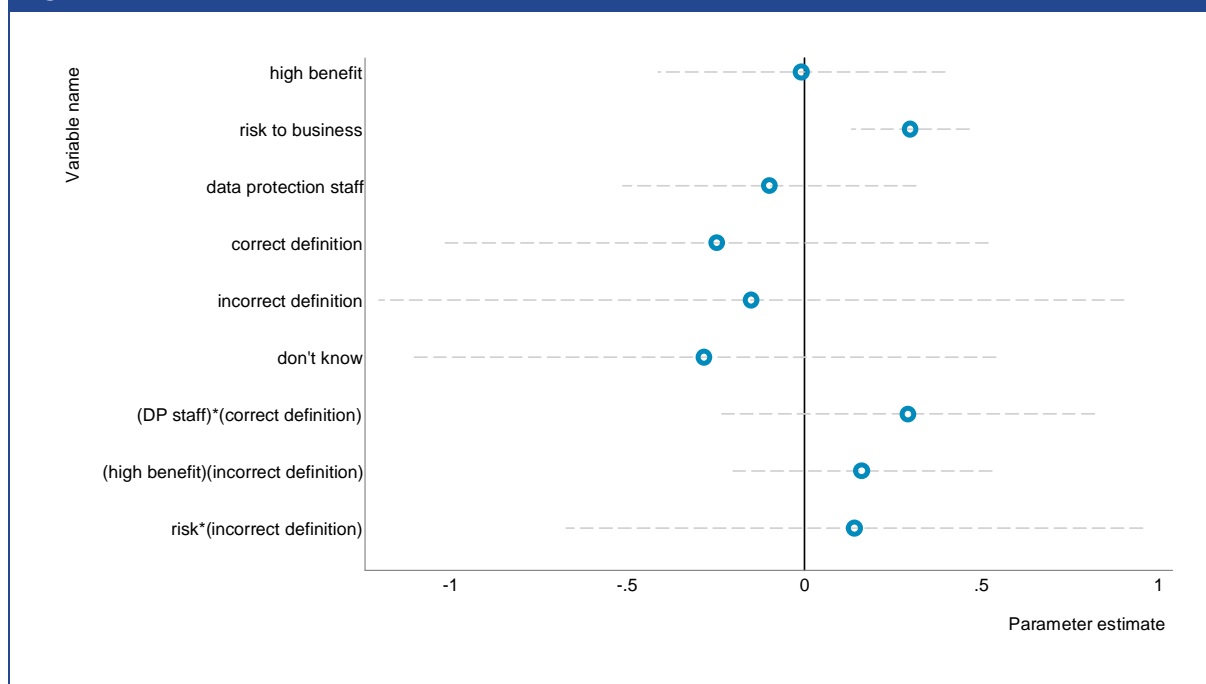


Source: London Economics

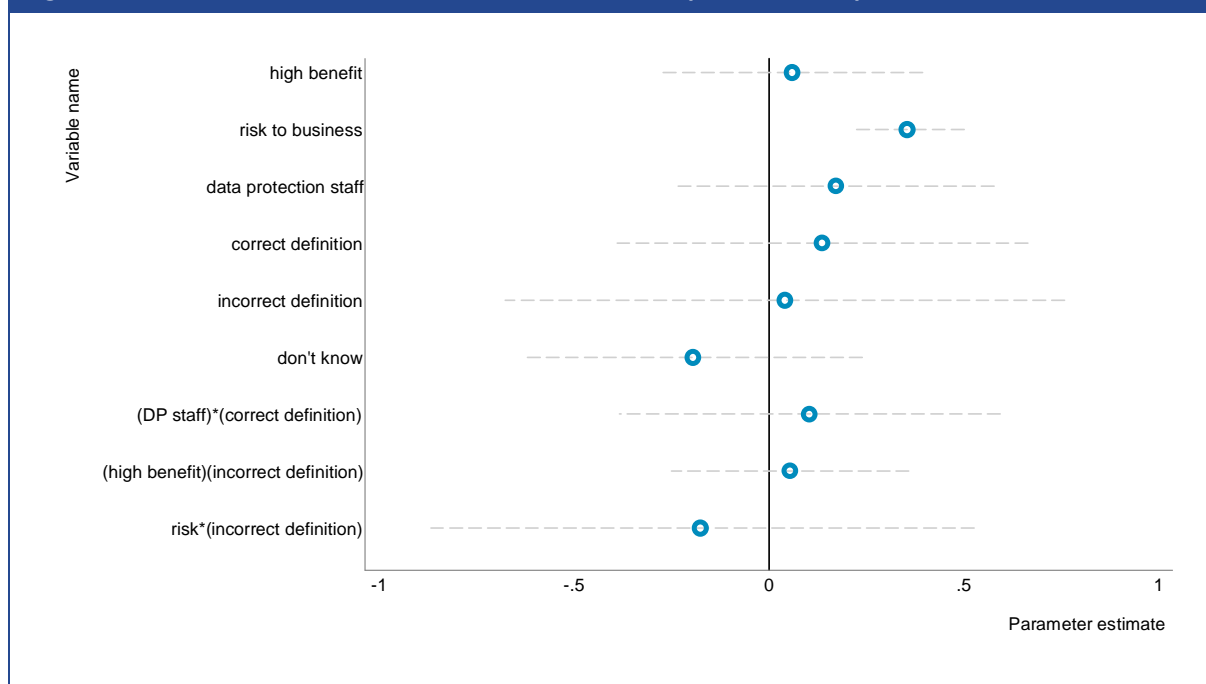
Figure 41: Predictors of additional cost related to data portability



Source: London Economics

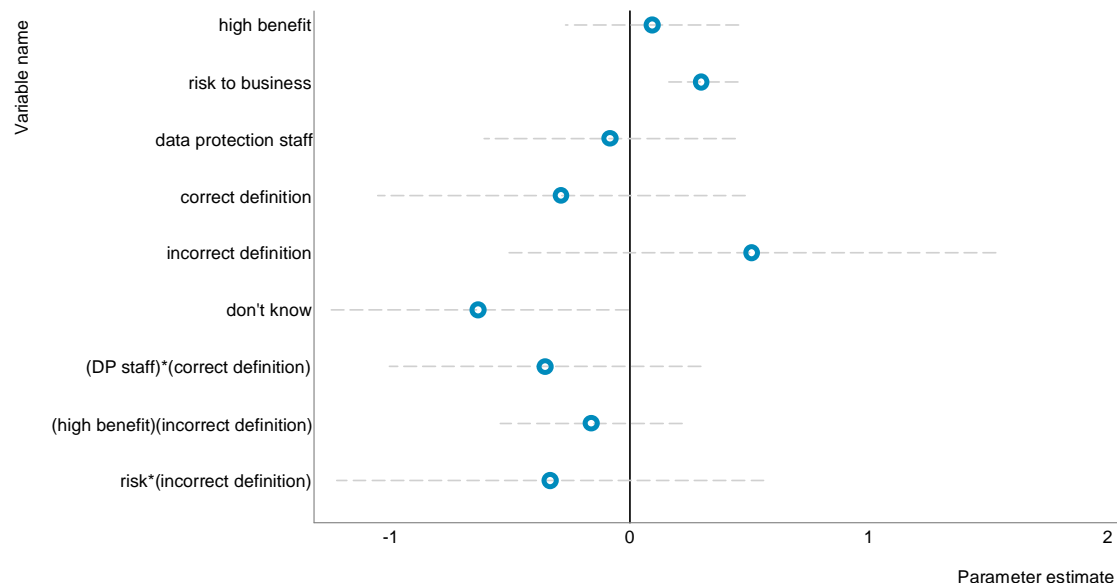
Figure 42: Predictors of additional cost related to breach notification

Source: London Economics

Figure 43: Predictors of additional cost related to data protection impact assessments

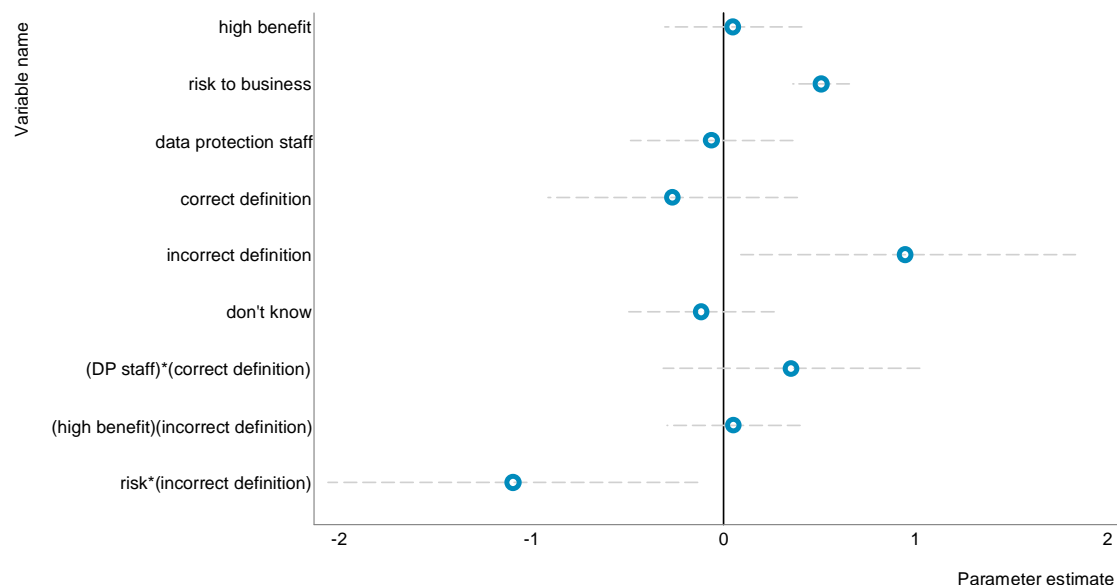
Source: London Economics

Figure 44: Predictors of additional cost related to data protection officers



Source: London Economics

Figure 45: Predictors of additional cost related to administrative sanctions



Source: London Economics

A1.4.3 Regressions by provision

Table 18: Regression output: expected additional cost of provision (1 = no additional costs; 5 = substantial additional costs)

Explanatory factors	Definition of personal data	Consent	Data minimization	SARs	Right to be forgotten	Data portability	DPOs	Breach notification	Sanctions	DPIAs
High benefit	0.0631 (0.164)	0.387** (0.158)	0.450*** (0.162)	0.0148 (0.169)	0.378* (0.211)	0.0951 (0.187)	0.0932 (0.184)	-0.00896 (0.205)	0.0513 (0.180)	0.0597 (0.170)
Risk to business	0.218*** (0.0652)	0.168*** (0.0629)	0.132** (0.0641)	0.272*** (0.0661)	0.284*** (0.0792)	0.288*** (0.0704)	0.300*** (0.0781)	0.299*** (0.0840)	0.508*** (0.0751)	0.355*** (0.0738)
DP staff	0.264 (0.219)	0.643*** (0.229)	0.630*** (0.196)	0.539*** (0.183)	0.374** (0.185)	0.359* (0.192)	-0.0830 (0.267)	-0.0988 (0.210)	-0.0613 (0.214)	0.172 (0.206)
Correct definition	-0.392 (0.364)	-0.156 (0.311)	0.199 (0.221)	0.0298 (0.243)	-0.181 (0.310)	-0.287 (0.253)	-0.286 (0.390)	-0.247 (0.389)	-0.266 (0.329)	0.137 (0.267)
Incorrect definition	-0.0512 (0.369)	0.437 (0.458)	0.262 (0.349)	0.326 (0.382)	-0.231 (0.420)	0.216 (0.427)	0.510 (0.518)	-0.150 (0.533)	0.949** (0.449)	0.0415 (0.364)
Don't know	0.0730 (0.319)	-0.342 (0.252)	0.343* (0.188)	-0.171 (0.188)	-0.339 (0.225)	-0.255 (0.206)	-0.635** (0.319)	-0.283 (0.418)	-0.115 (0.191)	-0.194 (0.220)
(DP staff)*Correct	0.555** (0.262)	-0.324 (0.277)	-0.0808 (0.220)	-0.108 (0.255)	0.246 (0.304)	0.166 (0.245)	-0.354 (0.331)	0.292 (0.267)	0.354 (0.339)	0.105 (0.248)
(High benefit)*Incorrect	-0.0358 (0.171)	-0.170 (0.127)	-0.106 (0.129)	0.251 (0.166)	-0.177 (0.198)	0.170 (0.181)	-0.162 (0.193)	0.161 (0.187)	0.0525 (0.176)	0.0546 (0.155)
Risk*Incorrect	0.109 (0.333)	-0.432 (0.444)	-0.0546 (0.347)	-0.345 (0.380)	-0.0556 (0.416)	-0.180 (0.418)	-0.332 (0.453)	0.141 (0.413)	-1.096** (0.488)	-0.176 (0.357)
Constant	1.446*** (0.228)	1.458*** (0.226)	1.552*** (0.219)	1.272*** (0.228)	1.443*** (0.256)	1.389*** (0.239)	1.416*** (0.281)	1.498*** (0.276)	1.188*** (0.248)	1.379*** (0.240)
Observations	259	263	253	246	233	231	242	236	228	232
R-squared	0.149	0.136	0.149	0.171	0.193	0.185	0.107	0.129	0.203	0.180

