Research and analysis to quantify the benefits arising from personal data rights under the GDPR

Report to the Department for Culture, Media & Sport

LE London Economics

May 2017

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 other 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.londoneconomics.co.uk.

Head Office: Somerset House, New Wing, Strand, London, WC2R 1LA, United Kingdom.

w: londoneconomics.co.uk e: info@londoneconomics.co.uk : @LondonEconomics
t: +44 (0)20 3701 7700 f: +44 (0)20 3701 7701

Acknowledgements

The research benefited greatly from DataIQ's help in facilitating contacts with senior data professionals in UK businesses.

Authors

Moritz Godel, Wouter Landzaat, James Suter

Table of Contents

Table of Contents

Executive Summary

Economic benefits arising from greater consumer trust in the digital economy are frequently cited in support of the European data protection framework in general, and the GDPR specifically. However, unlike with benefits for firms from reduced administrative burdens (one-stop shop, reduced notification requirement), these benefits have not been analysed in detail.

This study represents the most extensive direct attempt to characterise and measure the benefits the **rights of individuals** included in the GDPR, namely:

- The right of access one's personal data
- The right to erasure of one's personal data; and
- The right to data portability.

The value of GDRP rights for individuals

Individuals value their personal data and the value increases with the quantity and the sensitivity of the data involved.

The act of disclosing personal data typically takes place in an environment of incomplete and asymmetric information. This explains the crucial role of consumer confidence in enabling transactions that involve the disclosure of personal data.

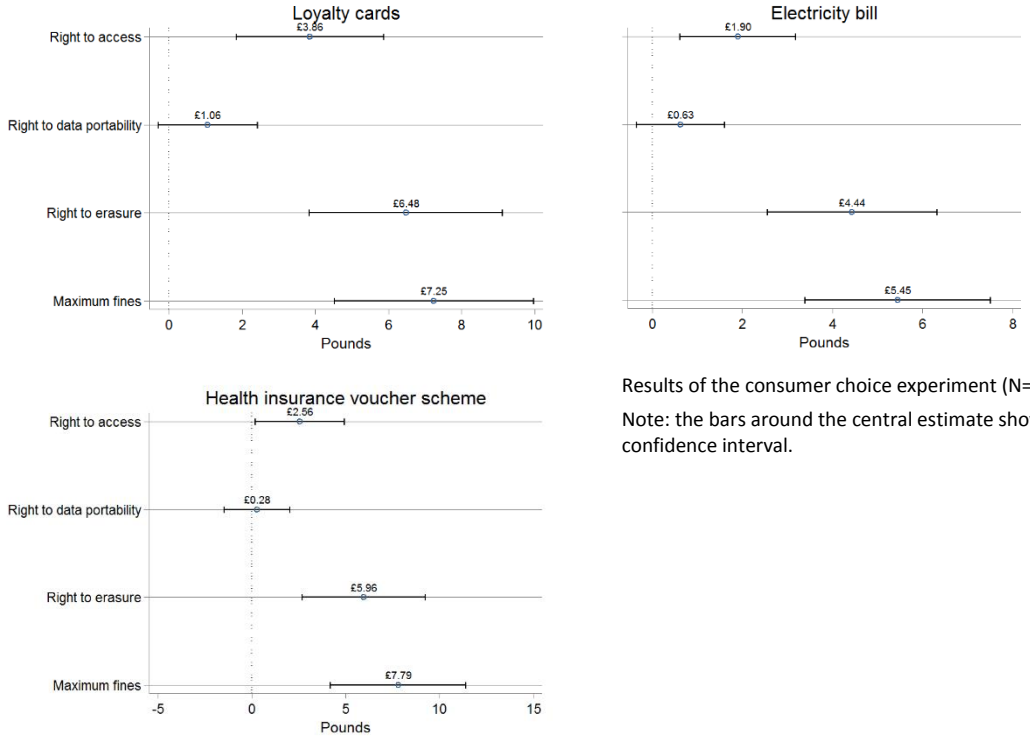
Despite widespread concerns about disclosure, **participation in digital markets is pervasive and rising.** Participation in digital markets is almost universal and non-participation is concentrated among older and socially disadvantaged demographics, which suggests a lack of resources and/or digital skills as more likely explanations than a lack of confidence in data protection. Moreover, data protection law is not well known, which makes it difficult to conceive of a strong incremental effect of GDPR.

This study uses a **choice experiment** to elicit realistic, context-specific valuations of GDPR rights for three common data-intensive transactions: retail store loyalty cards, electricity smart meters and rewards for health & lifestyle monitoring in health insurance contracts.

The consumer choice experiment finds that **individuals are willing to forego savings of roughly 5% to 10%** on weekly spending on shopping, monthly spending on electricity or monthly spending on health insurance in order to have the rights enshrined in the GDPR. This large valuation indicates that individuals are generally happy with the package of rights they have and that they should be compensated significantly for these rights to be taken away.

Furthermore, **the existence of maximum fines for non-compliance with the law is highly valued.** This high valuation may be interpreted as an implicit insurance against things going wrong. Individuals are willing to pay for the existence of punitive measures, which should deter non-compliance.

Consumer valuation of GDPR rights



Results of the consumer choice experiment (N=502)

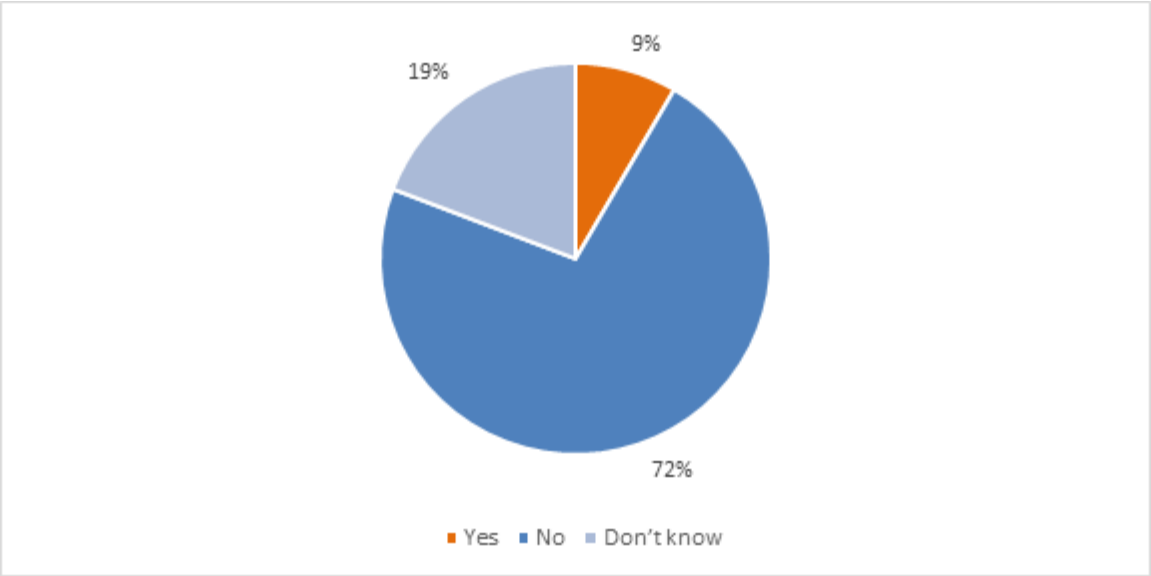
Note: the bars around the central estimate show the 95% confidence interval.

Source: LE survey of consumers (2017) Choice experiment

Data rights are seen by consumers as almost as important as brand reputation, past experience and the type of data involved in the decision to give out personal data, with data rights only seen as marginally less important. Consumers are more positive about how important data rights are in these decisions than professionals.

At the same time benefits to consumers are not necessarily predicted to translate to increased profitability of firms, both for specific benefits and rights and for the package of rights in general. **Only 21 of the 250 of the professionals surveyed predict that the package of rights to data portability, erasure and access will increase their profitability.**

Do you think that the availability of the right to data portability, access and erasure will increase the profits of your organisation?



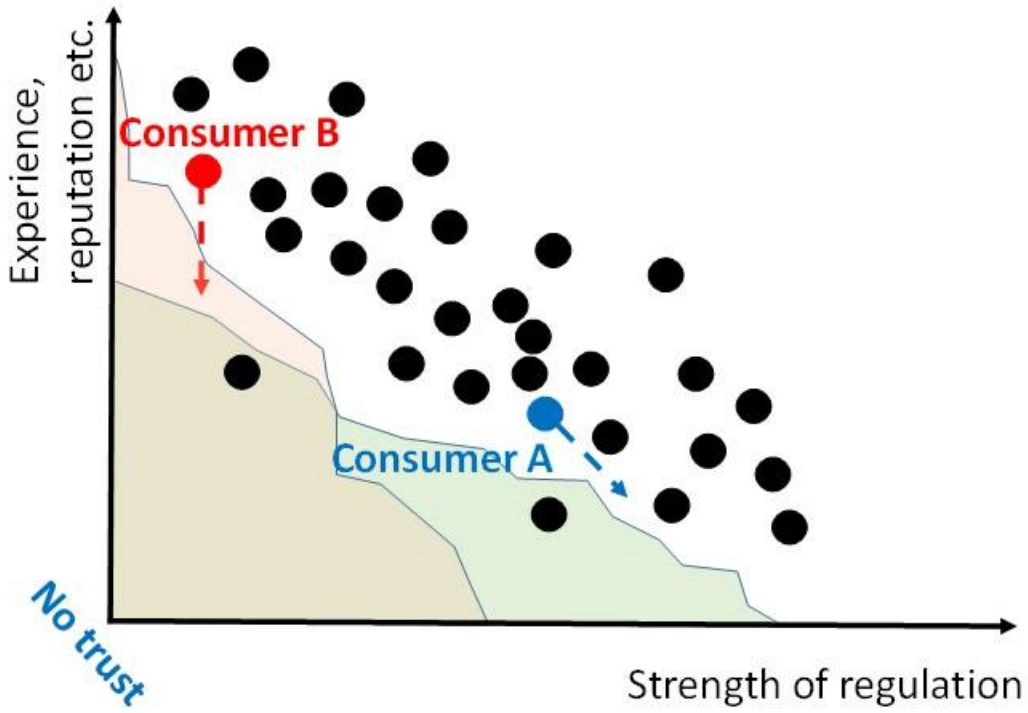
Source: LE survey of data protection professionals (2017)

Overall, data professionals show a **high level of uncertainty** when asked to assess the benefits of GDPR data rights. It is noteworthy that the in-depth interviews revealed a **lack of imagination and preparedness in terms of the more far-reaching impacts of GDPR,** especially second-order effects such as the emergence of new data-centric business models and privacy & and data protection as a competitive advantage.

This suggests that the value of the GDRP rights from consumers' point of view does not depend on consumers actively using their rights, but that more widespread awareness of the scope of personal data use might make the rights even more valuable in the eyes of consumers.

A stronger regulatory framework is likely to mitigate the effect of a localised loss of trust (i.e. a data breach affecting a specific data controller), by reassuring consumers that companies in general are incentivised (through rights that allow user control etc.) to keep data safe, and to react to a loss event by strengthening security.

GDPR rights as a safety net for digital markets



Note: Transactions can only take place outside the "confidence boundary" (the coloured area in the figure above). The location of the boundary can vary across consumers and across counterparties/transaction types. A loss of consumer trust based on the performance of the data controller such as a data breach results in some consumers falling below the minimum level of confidence needed to transact (Consumer B). A strong regulatory framework mitigates this loss of trust (Consumer A), so that transactions can continue to take place (or confidence recover more quickly).

Source: LE

This implies that the greatest benefit of the GDPR is not what it enables, but what it prevents, namely a collapse in confidence after the direct drivers of trust (above all consumers' experience of things not going wrong) have failed.

The hypothesis that a strong regulatory framework, including sanctions, acts as a backstop that enables customer confidence to bounce back after an incident is consistent with the evidence.

Benefits of key GDPR rights

Right of access

The GDPR brings an incremental strengthening of the **right of access.**

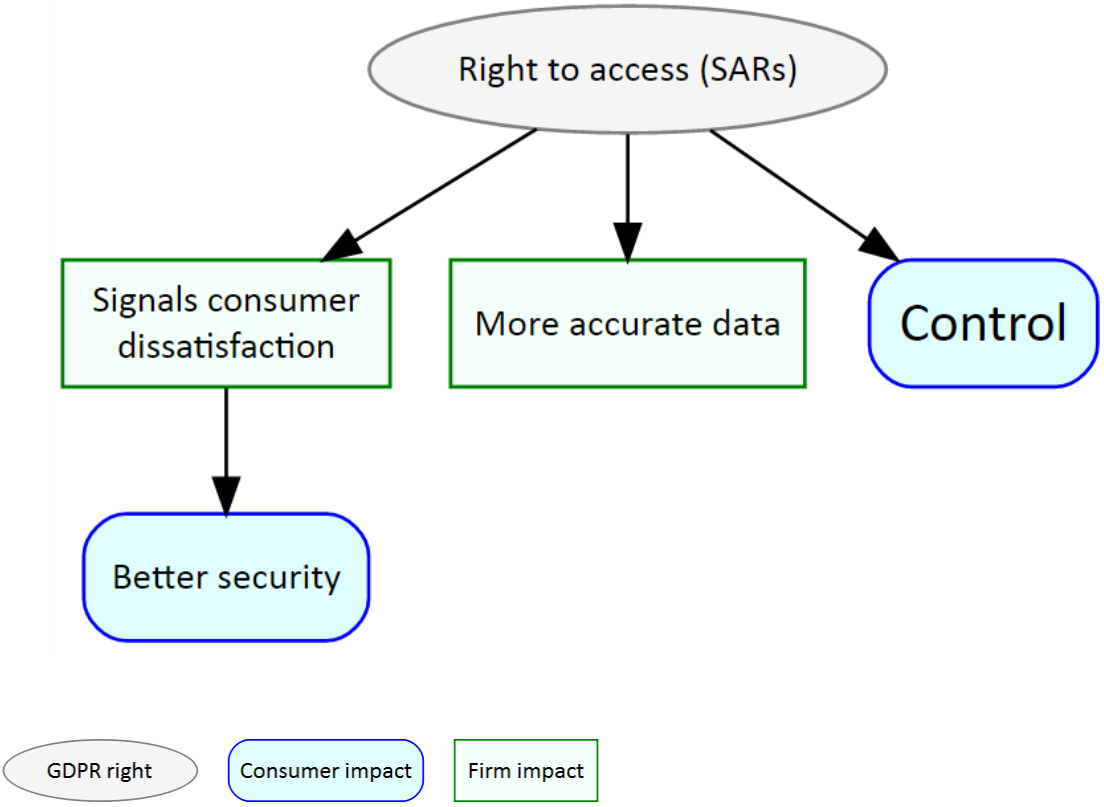
Greater control for consumers over their data is seen by professionals as the most likely benefit to occur, while more accurate data is seen as having the greatest potential impact on profitability for data controllers.

Access requests are interpreted by businesses as signals of consumer dissatisfaction. As such, they may incentivise good data protection practices.

There is a consistent discrepancy between the assessment of likelihood and the assessment of impact: The number of respondents that agree that agree or strongly agree that a benefit impacts

positively on profitability is consistently smaller than the number that see a benefit as likely or extremely likely.

Benefits arising from the right of access



Note: A larger font size in the node indicates that more data professionals indicate that they think a benefit is likely or extremely likely to occur.
Source: LE

Right to erasure

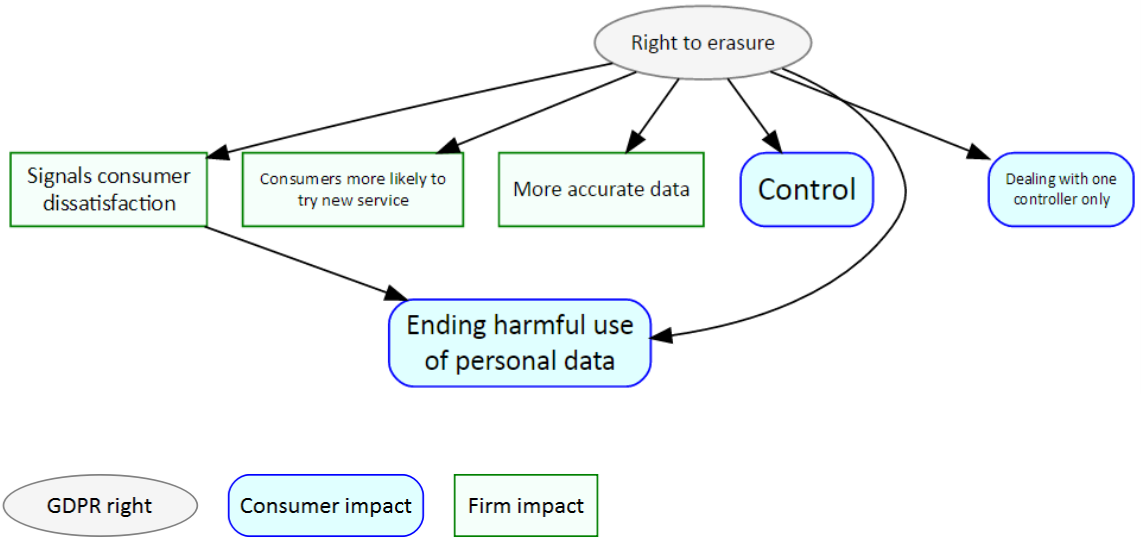
The **right to erasure** is a substantial change compared with the current legislation and is seen as an extension or further strengthening of the right of access.

The most likely benefits arising directly from the right to erasure are the end of harmful use of data and greater control of consumers over their data.

The right to erasure reflects consumer preferences and is seen as important in the decision to give out information.

Like access requests, requests to erase personal data are also seen as evidence of consumer dissatisfaction. There is little expectation that the right to erasure will be exercised often, driven partly by a lack of consumer awareness.

Benefits arising from the right to erasure



Note: A larger font size in the node indicates that more data professionals indicate that they think a benefit is likely or extremely likely to occur. Minimum font size has been set to 8 points for readability.
Source: LE

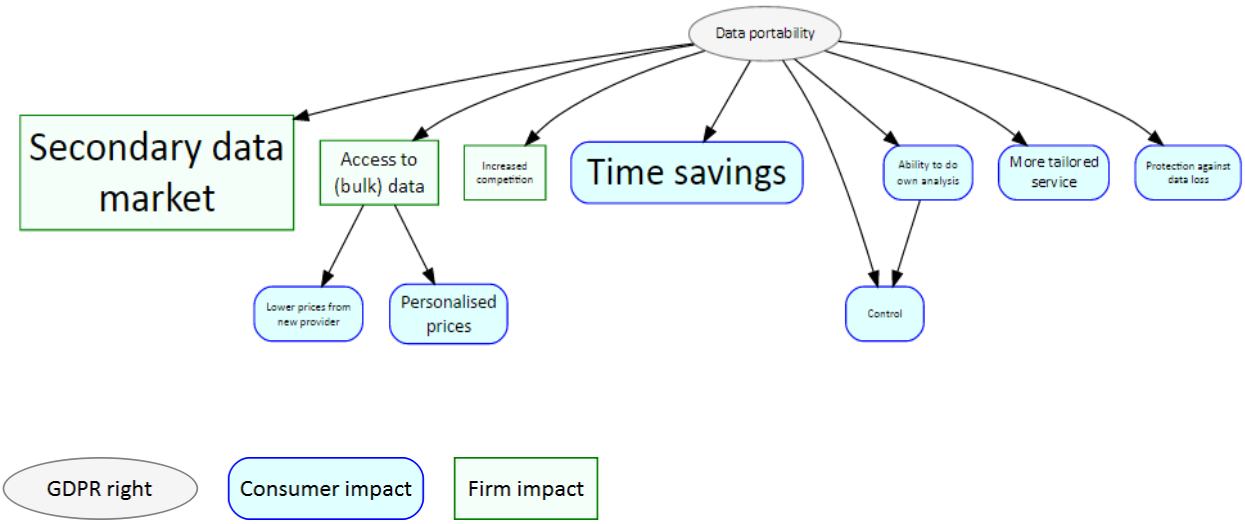
Data portability

The **right to data portability** is potentially the most far-reaching change from current legislation, and has the largest expected impact on the relation between data controller and consumer.

An increase in competition in markets that rely on the use of personal data is potentially the greatest source of benefit, but this does not come out strongly in the survey evidence. Uncertainty about the scope of the right and the new business models that may be enabled by the right make an assessment difficult.

Consumer switching – which data portability would enable – has been shown to be beneficial in different markets. Time savings and the existence of markets for secondary data are seen as the benefits most likely to arise.

Benefits arising from the right to data portability



Note: A larger font size in the node indicates that more data professionals indicate that they think a benefit is likely or extremely likely to occur. Minimum font size has been set to 8 points for readability.
Source: LE

Auxiliary rights

Data Protection Officers are seen as increasing awareness of and compliance with legislation. It is widely accepted that having a DPO does increase the status and priority of data protection within organisations. DPOs therefore have a positive impact on data security, quality and accuracy.

However, having a DPO is not seen to lead to lower costs for individuals wishing to exercise their data-related rights.

Consumers attach a higher value to the **existence of substantial fines** than to the other rights.

Professionals think that fines will have little extra impact on data security, but they may reinforce a security mind set in an organisation. The loss of consumer trust following a data breach is seen as a much larger problem for organisation than fines. Consumer trust is directly dependent on the data controller's performance with respect to security and not mediated through the level of fines.

1 Introduction

1.1 Background & context

Economic benefits arising from greater consumer trust in the digital economy are frequently cited in support of the European data protection framework in general, and the GDPR specifically. However, unlike with benefits for firms from reduced administrative burdens (one-stop shop, reduced notification requirement), no quantified estimates of these benefits have been provided in the official impact assessments[1].

Partly, this is because potential benefits are complex, including averted harm due to data minimisation and use limitation, direct benefits such as reduced transaction costs due to data portability and increased participation in online markets; and indirect benefits, notably higher security arising from stronger incentives for firms to keep data secure (fines, breach notifications) and increased competition (due to data portability and new customer segments entering digital markets for the first time).

> *"Businesses that fail to adequately protect individuals' personal data risk losing their trust. This trust, particularly in the online environment, is essential to encourage people to use new products and services."* EC (2016a)

Moreover, the benefits of trust are difficult to measure. While it is no doubt true that "trust (…) is essential to encourage people to use new products and services"[2]; the role of privacy and data protection in determining the level and intensity of consumer participation in online markets (and the resulting benefits in terms of lower prices/transaction costs and consumer choice) is still insufficiently understood.

A more detailed examination of the key provisions from an economic point of view is of substantial value to policymakers. Understanding the extent and the sources of economic benefit associated with the rights enshrined in the GDPR will be important for the further development of data protection policy and industrial strategy for the digital economy as well as operational priorities for the government (such as public awareness campaigns).

1.2 Objectives of the study

The aim of this study is to analyse and where possible to quantify the benefits arising from personal data rights under the GDPR. The focus of the study is on the **rights of individuals** included in the GDPR, namely:

- the right of access one's personal data
- the right to erasure of one's personal data; and
- the right to data portability.

Two **auxiliary provisions** supporting the effectiveness of the individual rights enshrined in the GDPR are also analysed:

[1] EC (2012), Ministry of Justice (2012).

[2] EC (2016b), p. 2.

- the requirement, under certain circumstances, to appoint a Data Protection Officer (DPO); and
- the increase in maximum administrative fines for infringements of data protection rules.

Other innovations of the GDPR, notably the new rules on consent, and the provisions that affect individuals only indirectly are outside the scope of this study.

1.3 Data sources

A review of secondary evidence, including surveys of public attitudes, trade publications and scientific literature was carried out alongside a multi-pronged primary data collection exercise. Primary data was collected through:

- an online survey of 250 individuals with data protection responsibility at their place of work (professionals survey);
- an online survey of 503 individuals including a choice experiment allowing for valuation of data rights (consumer choice experiment);
- three online forums with individuals with data protection responsibility at their place of work;
- seven in-depth interviews with senior data professionals in UK businesses.

Taken together, the exclusive focus of the research on the new GDPR rights (reflecting the most recent official guidance on content and scope), the use of sophisticated quantitative analysis of survey data (consumer choice experiment), and triangulation between consumer and industry perspectives the broader research literature on the economics of privacy and the role of trust in digital markets provide a new and substantive evidence base for thinking about the effects of GDPR. The report is structured as follows:

- Section 2 contains a brief review of attitudes towards data protection, participation in digital markets and the **potential benefits of GDPR rights.**
- Section 3: presents the results of the consumer choice experiments on the **valuation of GDPR rights.**
- Section 4: discusses the **benefits of individual GDPR rights** based on the survey of data protection professionals and secondary sources.
- Section 5: summaries the findings and presents a unifying **framework** for interpretation.

2 Benefits of GDPR: drivers & mechanisms

Box 1 Summary: Benefits of GDPR: drivers & mechanisms

Individuals value their personal data and the value increases with the quantity and the sensitivity of the data involved.

The act of disclosing personal data typically takes place in an environment of incomplete and asymmetric information. This explains the crucial role of consumer confidence in enabling transactions that involve the disclosure of personal data.

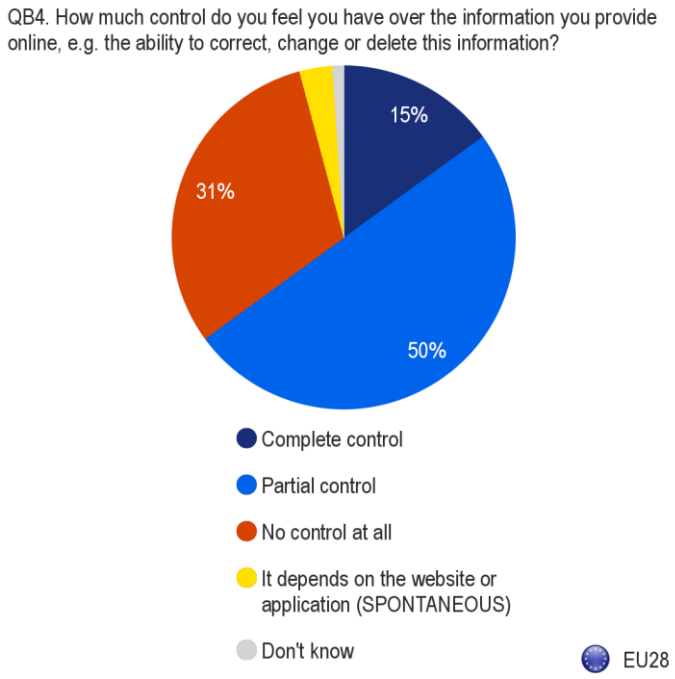
Impact assessments of the GDPR by the European Commission and the Ministry of Justice single out the increased market participation as a key benefit of enhanced consumer trust.

Despite widespread concerns about disclosure, participation in digital markets is pervasive and rising. Participation in digital markets is almost universal and non-participation is concentrated among older and socially disadvantaged demographics, which suggests a lack of resources and/or digital skills as more likely explanations than a lack of confidence in data protection. Moreover, data protection law is not well known, which makes it strong incremental effects of GDPR unlikely.

2.1 Consumer perceptions & privacy preferences

There is ample evidence that many individuals do not feel in control of personal data they disclose online and that they are concerned privacy and data protection when participating in the digital economy.

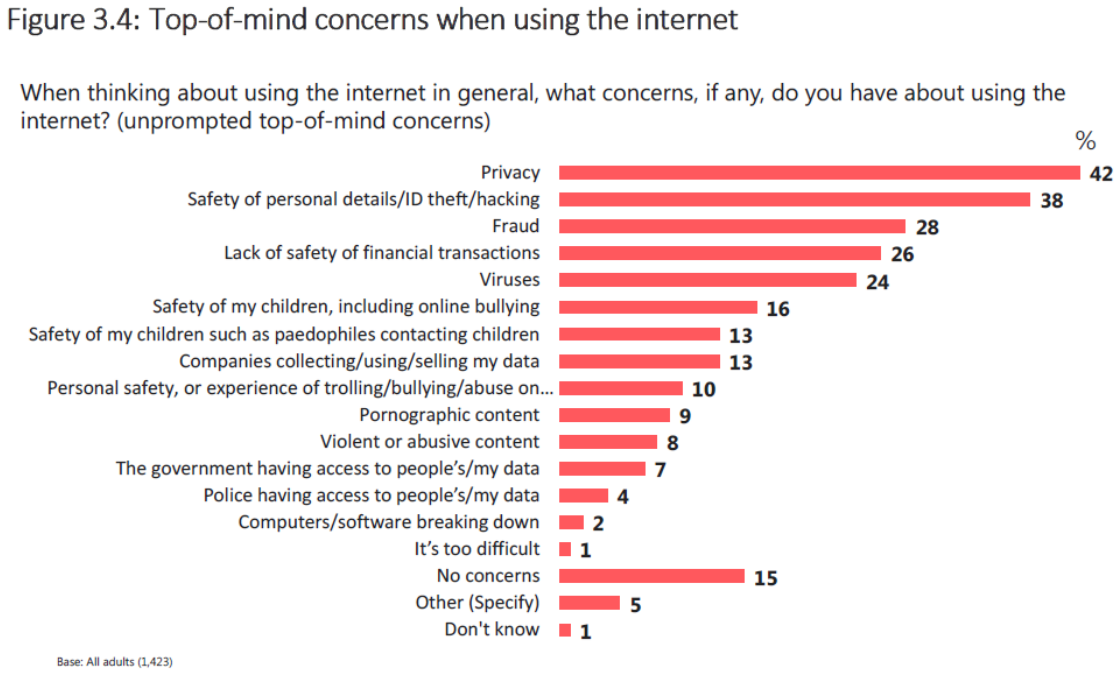
Figure 1 Control over information provided online



Source: Special Eurobarometer 431 (2015)

When asked about their concerns when engaging in online activities, 'privacy' is often cited as important, and sometimes as the most important factor (Figure 2).

Figure 2 Concerns when using the internet



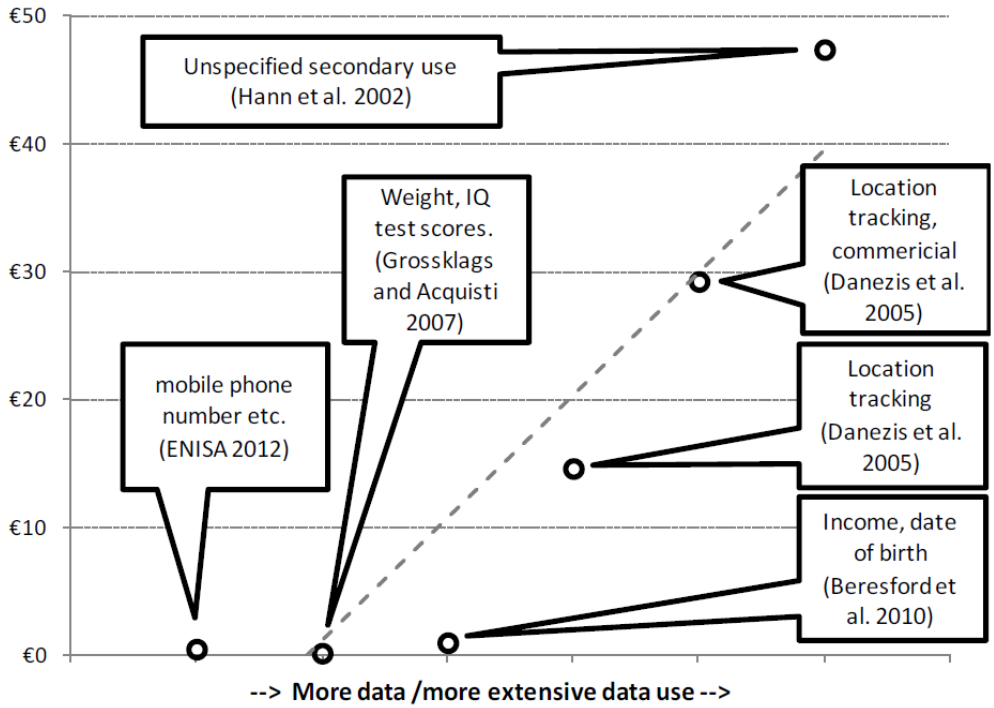
Source: Digital Footprints (2016)

While the reliability of self-reported privacy preferences needs to be interpreted with care due to the so-called **privacy paradox**[3] (in observed behaviour people often show less concern for privacy than surveys of attitudes and intentions would suggest), there is strong evidence for the basic fact that data protection is valuable to consumers, and that the valuation increases with the volume and sensitivity of data, as well as the scope of follow-on use once the data is disclosed.[4] Figure 3 illustrates the positive relationship between scope of processing and data type on the one hand and consumer valuation on the other.

[3] See Norberg et al. (2007).

[4] However, the monetary values reported in the economics literature are often suspect, see Godel et al. (2012).

Figure 3 Quantitative estimates of the value of personal data items in the economics literature



Source: Godel et al. (2012), p. 52.

2.2 Sources of benefit: the EC and MoJ impact assessments

Data protection law, and the new GDPR in particular, has been proposed as a key tool to aid the development of digital markets. The mechanisms through which this is thought to occur are: empowering consumers to exercise control over their personal data (and reducing the cost of exercising data protection rights); incentivising competition in markets that rely on the disclosure of personal data; and creating/safeguarding a climate of trust in which data-enabled exchanges can flourish.

The economics literature identifies several distinct economic benefits that result from the disclosure of personal information in digital markets, both for data controllers (savings, efficiency gains, surplus extraction, increased revenues through consumer tracking) and data subjects (personalised services, discounts from a loyalty program, targeted offers and promotions, reduced search costs and increased accuracy of information retrieval, etc.).[5] At the same time a lack of data protection is known to cause detriments, ranging from "costs incurred [by firms] when data is breached or misused, or collected in ways that consumers deem too intrusive" and identity theft, price discrimination, stigma or psychological discomfort for consumers.[6] Benefits turn into opportunity costs when individuals refrain from disclosing personal data. Disclosure (and non-disclosure) can also cause positive and negative externalities (social benefits/costs greater than the benefits/costs to an individual or firm involved in the transaction).

[5] See Acquisti et al. (2016), p. 462.

[6] Acquisiti et al. (2016), Tamir and Mitchell (2012), Stone and Stone (1990) and Feri et al. (2016).

The impact assessments carried out by the European Commission (EC, 2012) and the Ministry of Justice (MoJ, 2012) did not provide quantified estimates of benefits caused by new rights for individuals. However, qualitative arguments were made that identify an increase in market participation as the key driver of benefits on the consumer side. The EC impact assessment argued that:

*"Individuals are likely to encounter increasing problems with the protection of their personal data, or **refrain from fully using the internet as a medium for communication and commercial transactions.** The 75% of individuals currently not feeling in complete control of their personal data on social networking sites (and 80% when shopping online) is not likely to decrease without regulatory intervention which can support the confidence of individuals. Such a development could counteract the key performance target of the Digital Agenda for Europe for 50 % of the population to buy online by 2015."*[7]

The MoJ's impact assessment (2012) advanced a similar reasoning (albeit more focused on concrete harm to individuals):

*"Enhanced protection of personal data is a benefit to individuals who are less likely to be victims of identify fraud and can have more confidence sharing their data online. This may also have a knock-on economic benefit if it leads to an **increase in the use of internet services.** The Regulation also gives individuals greater control over their personal data through measures such as 'the right to be forgotten', and data portability."*[8]

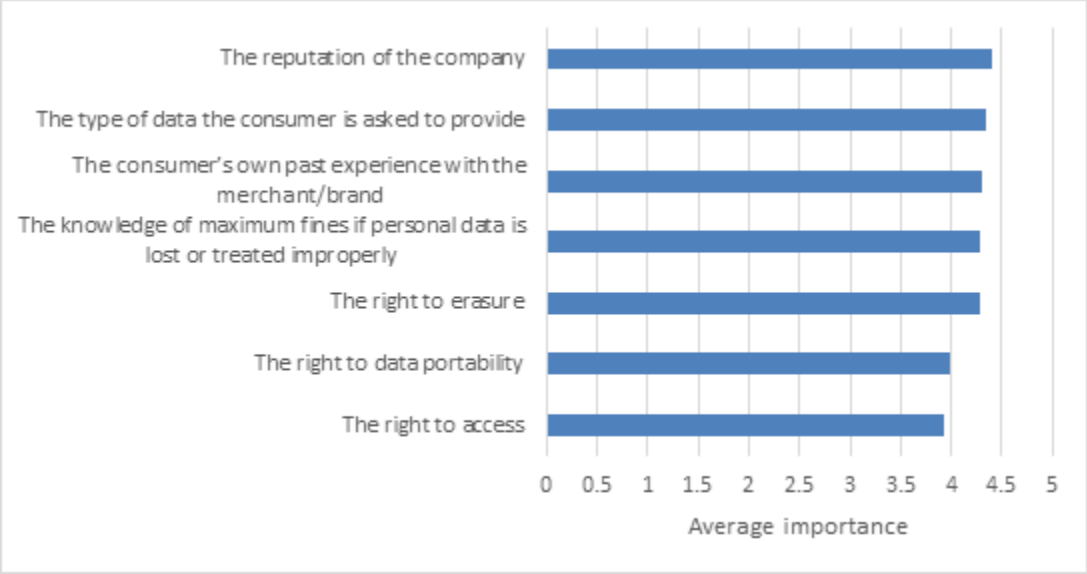
We summarise this line of reasoning about the benefits of GDPR as follows: Consumers' confidence when engaging in transactions that involve the disclosure of personal data depends on many factors, among them personal experience, the reputation of the counterparty (the data controller entrusted with the personal data) as well as the strength of the regulatory framework.

The consumer survey carried out for this study confirms that all of these factors play a role in consumers' purchasing decisions. Figure 4 shows the average importance that consumers attach to the different dimensions. The data confirms the importance of the different factors (including the different GDPR rights) and furthermore that they lie close together in terms of importance.

[7] European Commission (2012), p. 37.

[8] Ministry of Justice (2012), p. 1.

Figure 4 Average importance of different factors in the consumer's purchasing decision



Note: importance was ranked on a 1-5 scale.

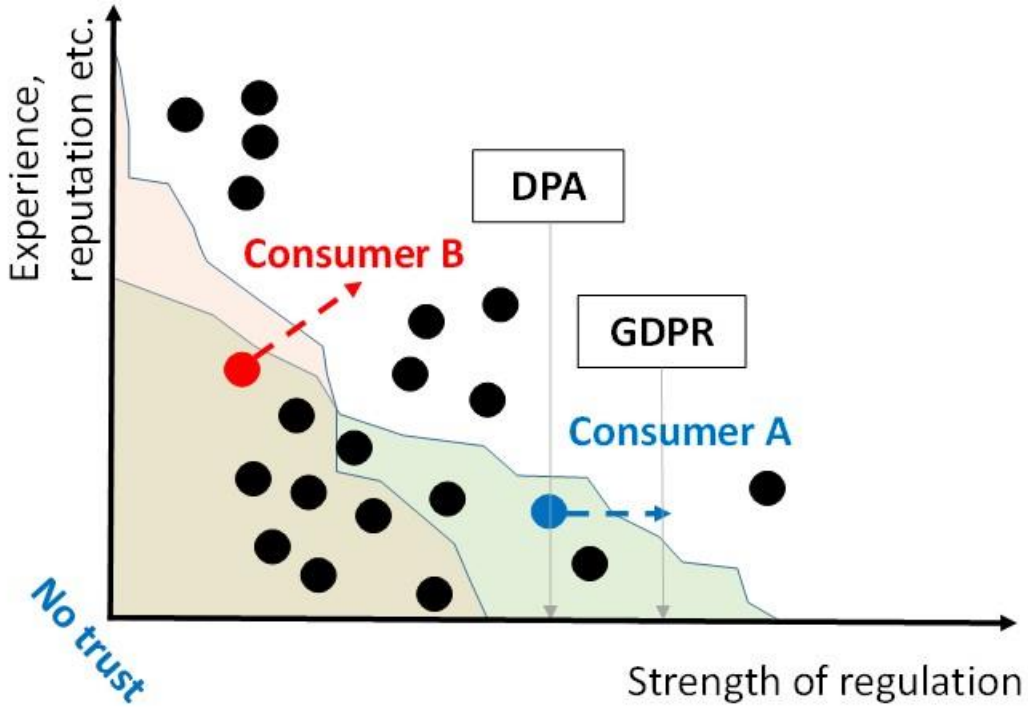
Source: LE survey of consumers (2017)

Confidence can come from the strength of the regulation (as the context in which trust is given) as well as from the consumer's own experience, the reputation/brand of the counterparty[9], etc. The confidence boundary demarcates the level of confidence necessary for transactions to take place[10].

[9] "(…) more than 75% of consumers are more willing to share personally identifiable information (PII) with brands that they trust than those they don't know (…). https://www.ama.org/publications/eNewsletters/Marketing-News-Weekly/Pages/Data-Sharing-Cheat-Sheet-Columbia-Business-School.aspx

[10] One interesting modification suggested by one respondent (representing a major retailer) was that GDPR might shift the confidence threshold outwards, by making issues of data protection more salient to consumers.

Figure 5 GDPR as a driver of consumer confidence



Note: Transactions can only take place outside the "confidence boundary" (the coloured area in the figure above). The location of the boundary can vary across consumers and across counterparties/transaction types

Source: LE

For consumers inside the boundary, a strengthening of the regulation can increase confidence sufficiently to get to a point beyond the boundary, where transactions are possible (Consumer A). In reality, a situation like that of Consumer B, in which a multi-dimensional pull on confidence enables the transaction is more likely (see Figure 4).

Note that the calculus is context-dependent (indicated by the differently shaded boundaries in the figure above), which makes general conclusions (including a potential quantification of total benefits from personal data rights) difficult to draw. What constitutes sensitive information, and the value associated with disclosure varies across individuals and use cases.[11]

However, a number of considerations cast doubt on this view of GDPR as a driver of economic benefits.

[11] Acquisti et al. (2016), p. 446: "Different pieces of information will matter differently to different people (your piano teacher may not be as interested in the schools you attended as your potential employer). The value of information will change over time (an online advertiser may not be as interested in logs of your online activity from five years ago as in your activity right now). In fact, the value and sensitivity of one piece of personal information will change depending on the other pieces of data with which it can be combined (…)".

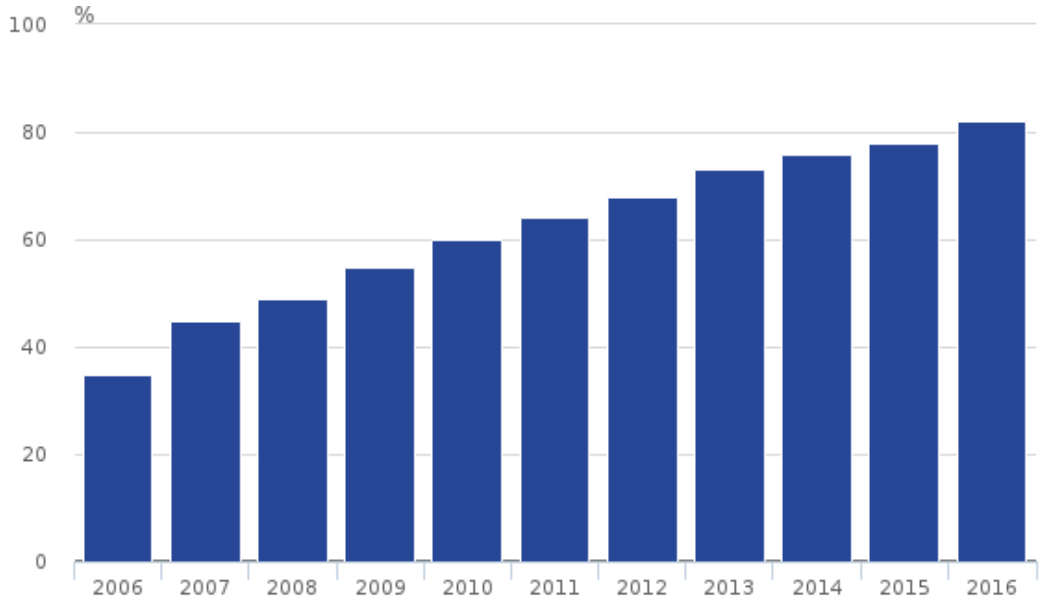
2.2.1 Caveats

Participation in digital markets is increasing

The scenario described by EC, where not implementing the GDPR ("regulatory intervention which can support the confidence of individuals" would "counteract the key performance target of the Digital Agenda for Europe for 50 % of the population to buy online by 2015" has not come to pass: the EC's own data shows that the target had been achieved by 2015: "Over the last five years, the number of European citizens ordering goods and services online has increased by 13 percentage points, to 53 %."[12]

Similarly, the increase in the use of internet services that was posited as a potential benefit of *enhanced* protection of personal data according to the MoJ is cannot be easily reconciled with a situation in which internet use in the UK has been growing consistently and is already very widespread: The internet was used daily or almost daily by 82% of adults in Great Britain in 2016, compared with 78% in 2015 and 35% in 2006. In 2016, 89% of households in Great Britain had internet access, and 77% of adults bought goods or services online.

Figure 6 Daily internet use by adults, 2006 to 2016, Great Britain



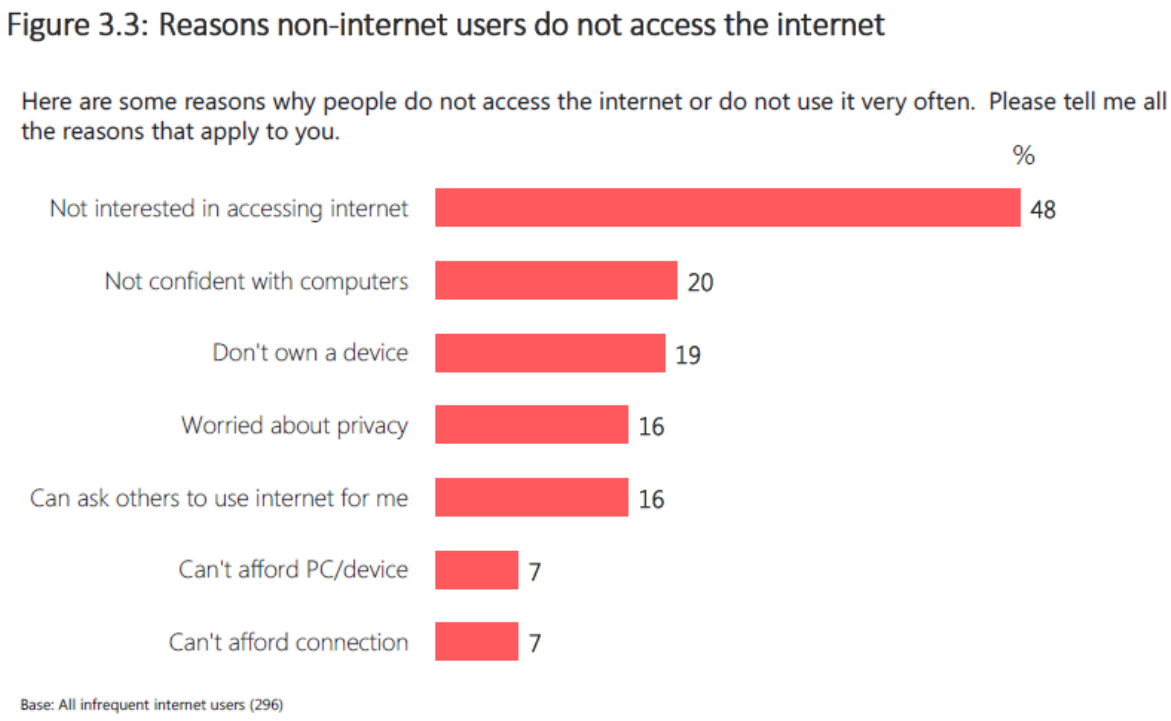
Note: Base: Adults aged 16+ in Great Britain

Source: Office for National Statistics, Internet Access Survey (2016)

Moreover, the available evidence suggests that a lack of data protection rights is not what is stopping the small minority of individuals that still do not participate in digital markets. A lack of interest and relevant skills as well as economic constraints have empirical support as alternative explanations for non-participation.

[12] European Commission (2016a).

Figure 7 Reasons why not to access the internet



Source: Digital Footprints (2016)

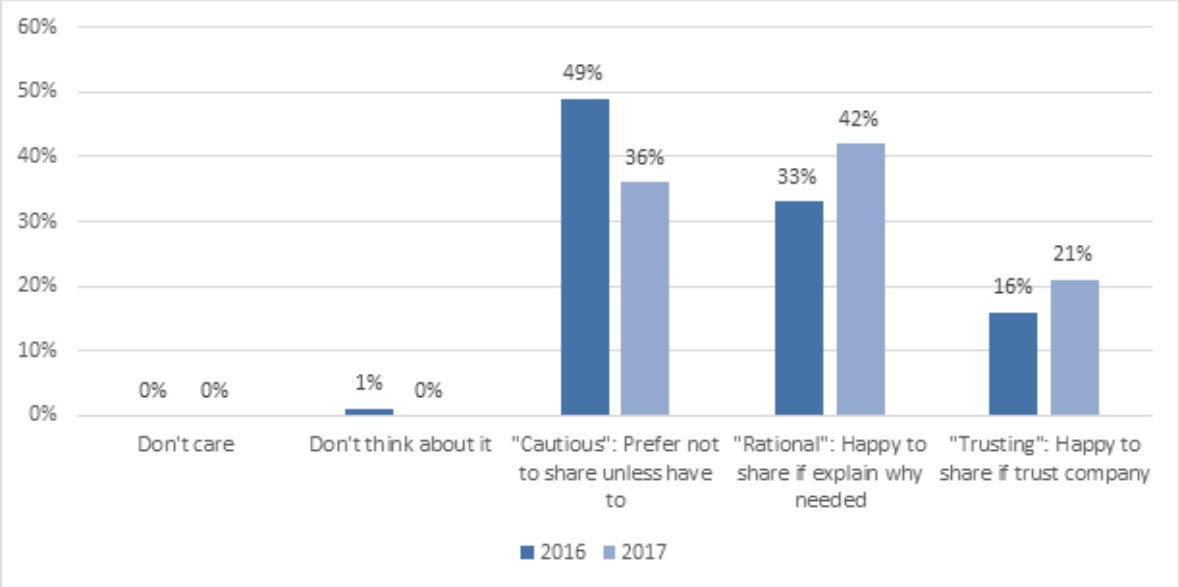
Moreover, the problem of non-participation is heavily concentrated among older people (nearly half of single pensioners have no internet access[13]), which suggests that it will continue to decline over time.

In addition, recent survey evidence[14] suggests that trust levels in the UK have in fact increased over the most recent period (Figure 8), which is consistent with the observed growth in the digital economy.

[13] Office for National Statistics, Internet Access Survey (2016). Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016

[14] DataIQ (2017). The results are based on 2 waves of an online survey (1,001 responses in 2016 and 1,000 in 2017) using representative of the adult (18+) UK population.

Figure 8 Consumer attitudes towards sharing personal information



Source: DataIQ (2017), Figure 1.1, p. 6

While the evidence discussed above is not conclusive (and does not take into account pull factors, such as the increasing range and attractiveness of digital offers, falling hardware costs, improving digital skills, etc.), it does contradict a simplistic view that that the key benefit of GDPR is that it increases participation in digital markets (either by people participating for the first time or by intensifying the participation of existing users). This does not mean that an unreformed data protection regime has not held back certain developments, or that it would not lead to problems further down the road. Furthermore, the argument that the debates around GDPR over the last years, which attracted considerable publicity, themselves contributed to greater consumer trust cannot be wholly dismissed.

GDPR represents an incremental change to an already strong data protection framework

In order to claim that the GDPR improves welfare for consumers through increased trust, we would need to show that a) current framework is a low trust environment (i.e. the DPA/Directive 95/46 does not engender sufficient trust) compared with GDPR and that b) the incremental changes in the GDPR improve trust[15].

However, the GDPR builds on the existing data protection framework (the DPA). Many key provisions, including the right of access and the right to erasure, exist already, albeit in weaker form. The GDPR thus represents a largely incremental change. This limits the incremental impact on consumer behaviour that can be expected as a result of the new rights enshrined in the GDPR.

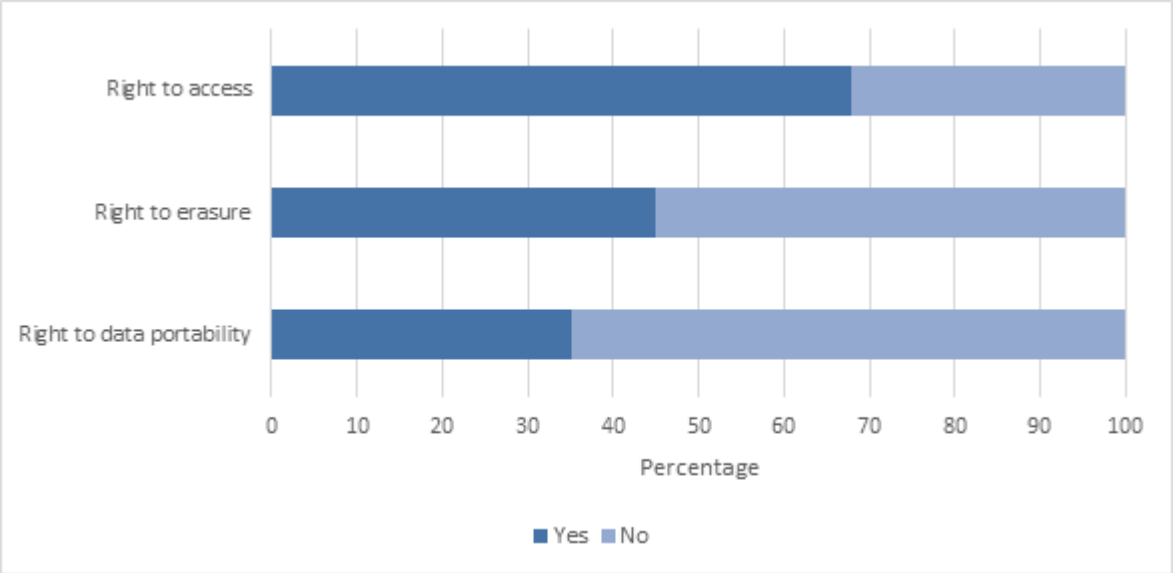
[15] LE (2012) strongly suggests that consumers are not aware of incremental changes in the law, so any effect is bound to be small.

Awareness of data protection rights is limited

This problem is exacerbated by widespread ignorance of the prevailing regulatory framework, demonstrated for example by LE's 2013 report for the ICO[16]. The consumer survey carried out for this study provided further evidence that knowledge of GDPR provisions is far from universal (and typically lower that digital market participation rates).

Figure 9 shows the percentage of survey respondents that are aware that they have the rights given to them in the GDPR. Most people (68%) are aware they have the right of access their data but only a minority are aware of the existence of the rights to erasure (45%) and data portability (35%).

Figure 9 Are you aware that you have the following rights regarding your personal data that organisations may hold on you



Source: LE survey of consumers (2017)

The incremental nature of GDPR, building on a largely functional and internationally respected data protection framework, together with limited awareness of some of the key data protection rights for individuals suggests that the effect of GDPR may not be large.

Digital markets can thrive outside the European data protection framework

A look at digital markets outside the EU casts further doubt on the idea that a lack of trust in the data protection framework is holding back data-driven transactions: For example, that almost a third of Americans trust European standards *more than American standards* when it comes to data privacy may suggest that a trust-enabled digital economy faces greater obstacles in the USA, other things being equal, even if cultural preferences for data privacy were stronger in Europe.

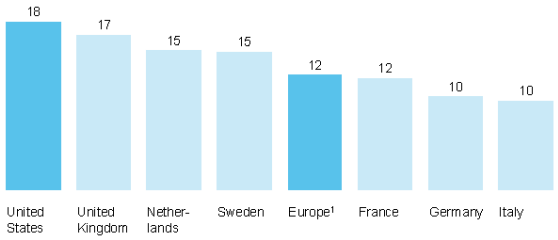
[16] When asked to identify 10 key GDPR provisions, 40% of 506 respondents (individuals with data protection responsibilities in UK organisations) had inaccurate knowledge of all 10 provisions considered. None of the survey respondents accurately described all 10 provisions. (The 10 provisions, based on the GDPR proposals, were: subject access requests; breach notification; data protection impact assessments; DPOs; fines; the 'right to be forgotten'; data portability; definitions; consent; and data minimisation.)

Figure 10 Trust in data privacy standards in Germany and the USA (2014)

Source: Pew Global Attitudes & Trends Question Database, "U.S.-Germany 2014", http://www.pewglobal.org/question-search/?qid=1762&cntIDs=&stdIDs=

However, Europe as a whole lags behind the USA on a broad range of digital economy indicators, which suggests that different data protection regimes are compatible with highly developed digital markets.

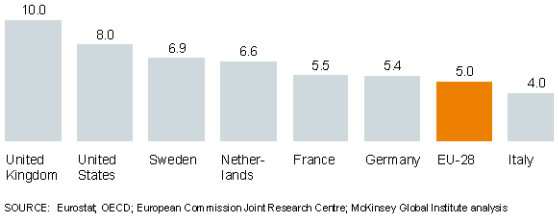
Figure 11 Captured potential of digitisation



Note: 1) Europe is the weighted average of the six countries shown here. These six countries make up 60% of the population, and 72% of GDP, in the EU-28 grouping.

Source: McKinsey Global Institute (2016), Exhibit 5, p. 12.

Figure 12 Digital Share of the economy (%)



Source: McKinsey Global Institute (2016), Exhibit 9, p. 18

The evidence that the US combines lower trust in the domestic data protection regime with a higher level of digital development does not support the view that the European digital economy suffers in comparison *because of* an insufficiently strong regulatory framework.

2.3 Conclusion & and implications for the study

The considerations above show that trust in digital markets is important, and that the trust deficit is real. However, the hypothesis that the mechanism by which the GDPR will produce benefits is through increasing consumer trust leading to increased participation in digital markets is at odds with the evidence of widespread and still increasing participation in digital markets. Moreover, the incremental nature of GDPR combined with limited knowledge of the details of the law makes large additional benefits less likely.

This study expands the knowledge base in two ways: First, a realistic, context-specific valuation of individual GDPR rights is currently not available. This study remedies this by undertaking the first rigorous attempt to measure the consumer valuation of individual GDPR rights (Section 3), using state of the art methodology to minimise respondent bias (the privacy paradox). Secondly, the mechanism through which GDPR produces benefits need to be better understood. Based on primary data collection among UK data protection professionals, we identify the key mechanism through which individual GDPR rights produce benefits (Section 4).

3 Consumers' valuation of GDPR rights

Box 2 Summary: Consumers' valuation of GDPR rights

A choice experiment is used to elicit realistic, context-specific valuations of GDPR rights for three common data-intensive transactions: retail store loyalty cards, electricity smart meters and rewards for health & lifestyle monitoring in health insurance contracts.

The choice experiment methodology mitigates bias in self-reported privacy preferences by presenting subjects with realistic and salient trade-offs across the relevant dimensions of the transaction, including price and data protection rights available to the subject.

To have the right of access or erasure, and for the existence of maximum fines consumers are willing to forego, for each right, roughly 5% to 10% of savings on transactions requiring transfers of data.

Survey evidence shows a) that consumers show significant gaps in awareness of the extent to which personal data is collected as part of common transactions, and b) that GDPR rights are unlikely to be exercised frequently.

This suggests that the value of the GDRP rights from consumers' point of view does not depend on consumers actively using their rights, but that more widespread awareness of the scope of personal data use might make the rights even more valuable in the eyes of consumers.

3.1 A choice experiment to elicit valuations for GDPR rights

Establishing how much consumer value the individual rights enshrined in the GDPR is difficult: since the GDPR is not yet in force, we have to rely on stated preferences, which is problematic because people overstate their concern for privacy relative to their revealed preferences (the privacy paradox). Moreover, as valuation is context-specific (certain types of data are more sensitive than others), a realistic valuation needs to be based on specific transactions, where both the type of data, its use by the data controller and an approximate underlying value range are known. Finally, the content and scope of the rights to be investigated need to be made explicit to overcome the problem of low levels of awareness of the content of the GDPR.

To address these issues as far as possible, a series of choice experiments has been conducted to obtain realistic valuations for the GDPR rights. In a choice experiment, subjects are presented with a set of binary choices between multi-attribute scenarios, in which the attributes are varied so as to force subjects to make trade-offs. A well-designed choice experiment can provide a more accurate estimate of consumer value than survey evidence because it is putting the subjects into real choice

situations, where attribute combinations can be compared directly and preferences are revealed through the observed choices[17].

The first step in the design of the choice experiment was the choice of appropriate transactions (contexts). Three contexts were chosen, with familiarity to consumers as the main criterion: The first context was a **loyalty card scheme,** the second context was the use of **smart meters** and the third context was a voucher programme run by a **health insurance** company. In each context, consumers were asked to make a number of choices between two loyalty schemes, smart meters or voucher schemes with varying attributes in terms of the rights provided with them and the discount they would receive for providing context-specific personal data. Expenditure and discount levels were set with reference to measured household expenditure and evidence from market reports about the discount levels available for existing loyalty schemes.

In each context, subjects (a random sample of 502 UK adults from the YouGov consumer panel) were presented with choices between two options, where a discount could be received in return for personal data. Each option varied in terms of the average (weekly or monthly) discount the individual would receive on their bill and on the personal data rights they would be given as part of the package. More specifically, the attributes varied were:

- the average discount (£),
- whether the right of access was granted,
- whether right to data portability was granted,
- whether the right to erasure was granted, and
- whether there was a maximum fine for non-compliance[18].

In all cases, both options could be refused by respondents. The results show that individuals are prepared to trade personal data and data rights in economic transactions if they are compensated sufficiently.

As an additional measure to ensure that the choice experiment provides evidence with real-world importance, respondents were asked to rate the realism of the experiment. Most choices (77%) were made by people who felt they could make at least somewhat realistic choices, whereas around 20% of choices under seemingly fully realistic conditions. This indicates that the choice experiment provided realistic scenarios and results should not be discounted on the basis of unrealistic framing.

3.2 Results of the choice experiment

3.2.1 Loyalty card scheme

The first context in which consumers made decisions was a loyalty card scheme where, in return for personal data, individuals can obtain a discount on their weekly shopping for food and drink.

The results are shown in Figure 13. The average value to consumer for the rights and maximum fines ranges from approximately £1 to £7.25. This translates into roughly 5% to 10% of weekly shopping. These values are rather high – with the exception of the value for data portability – which indicates

[17] See Annex 2 for further details on methodology.

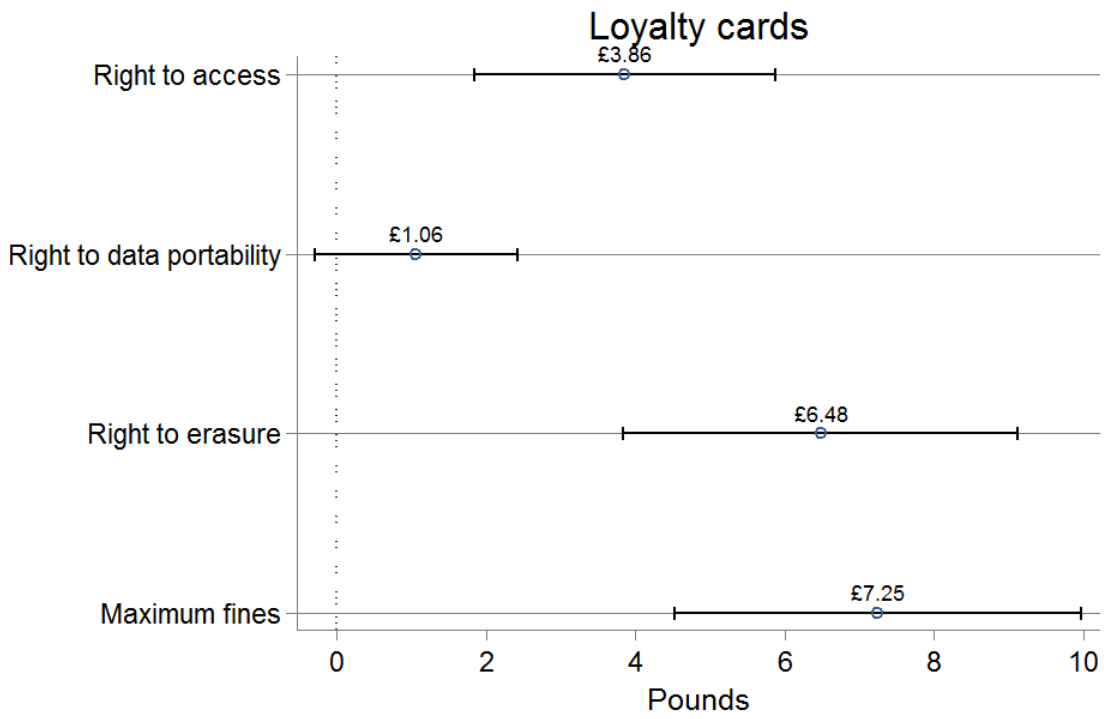
[18] The options for the maximum fine were either "Zero" or "£15 million or 5% of turnover, whichever is greater". These numbers are deliberately different from the maximum fine established in the GDPR.

that people are happy with the set of rights they have, and they should be thoroughly compensated if the rights were to be taken away. The high value for the existence of fines can be interpreted as an insurance on data breaches. People are effectively willing to pay £7.25 per week for the existence of punitive measures if things go wrong.

The numbers represent the consumer valuation of the GDPR rights in the context of transactions that they are already prepared to engage in (rather than an additional value created by the GDPR). As such, they point to the role of the data protection framework as underpinning the market as it is, rather than a future market equilibrium.

The estimates are the result of a context-specific, detailed choice scenario in which the relevant factors (the right-discount trade-off) are made highly salient and with which consumers are familiar. Moreover, discount ranges and weekly expenditures are calibrated to reflect actual patterns in household consumption and discounts offered by supermarkets. The estimates represent the best evidence so far that specific GDRP rights confer substantial benefits to consumers, which can be quantified in money terms.

Figure 13 Consumer valuation of GDRP rights: loyalty cards



Note: the bars around the central estimate show the 95% confidence interval.

Source: LE survey of consumers (2017) Choice experiment

Table 1 provides a numerical summary of the average consumer valuation for rights or the existence of a maximum fine[19] in absolute terms in in relation to weekly spend.

Table 1 Average value to consumers of rights and fines, in the loyalty card context

	Value in £	Value as percentage of weekly spending on shopping
Right to request complete details of the personal data the provider has on you	3.86	6%
Right to copy or transfer your personal data from the current provider to another	1.06	2%
Right to request the deletion or removal of personal data stored by the provider	6.48	10%
Provider faces a fine of £15m or 5% of turnover for non-compliance	7.25	11%

Note: Average total weekly shopping expenditure in the survey is £67.19.

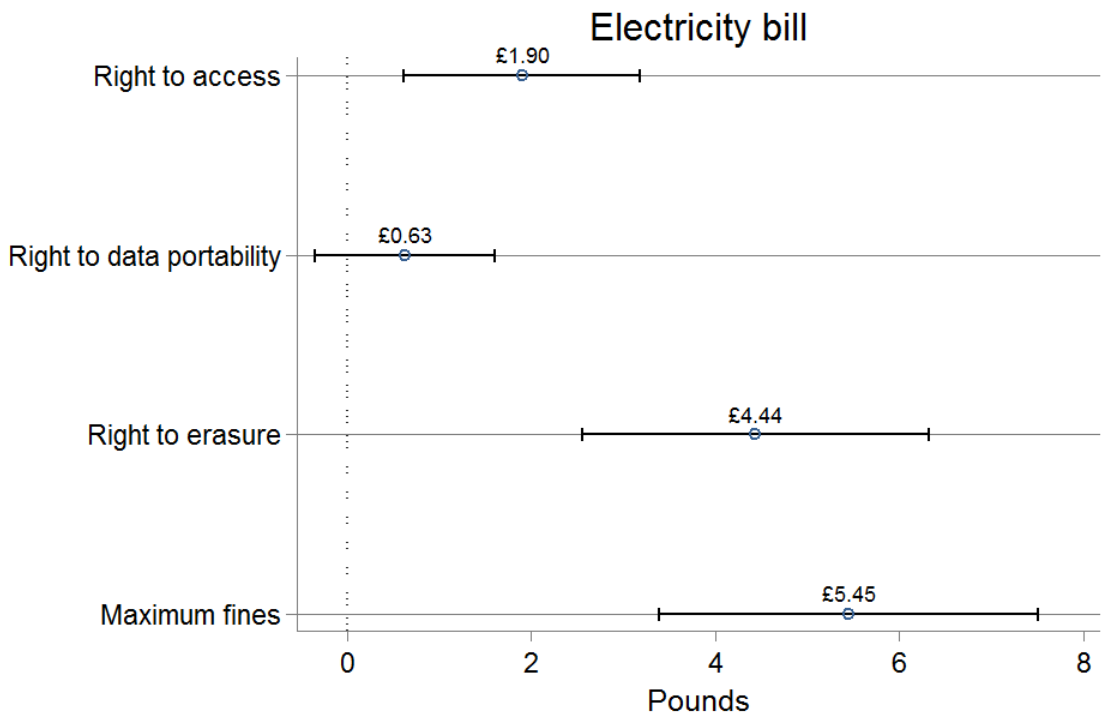
Source: LE survey of consumers (2017) Choice experiment

3.2.2 Smart meters

The second context in which consumers made decisions is the use of smart meters. Smart meters provide discounts on one's monthly electricity bill but in return they allow the supplier to collect personal data on individuals.

[19] The "valuations" are the amounts that consumers are willing to forego (i.e. WTP) in terms of savings on their weekly food and drink shopping, in return for the right in question. A higher valuation implies that consumers should be compensated more by businesses if their rights were to be taken away, and therefore indicates higher satisfaction with their rights.

Figure 14 Consumer valuation of GDRP rights: smart meters



Note: the bars around the central estimate show the 95% confidence interval.

Source: LE survey of consumers (2017) Choice experiment

Average valuation, which in this case is the average monthly savings they are willing to forego to be granted a given right is presented in Table 2 in absolute and relative terms.

Table 2 Average value to consumers of rights and fines, in the smart meter context

	Value in £	Value as percentage of monthly spending on electricity
Right to request complete details of the personal data the provider has on you	1.90	4%
Right to copy or transfer your personal data from the current provider to another	0.63	1%
Right to request the deletion or removal of personal data stored by the provider	4.44	8%
Provider faces a fine of £15m or 5% of turnover for non-compliance	5.45	10%

Note: Average total monthly expenditure on electricity in the survey is £52.80.

Source: LE survey of consumers (2017) Choice experiment

The average consumer value ranges from £1.90 to £5.45[20]. This translates into roughly 5 to 10% of the monthly electricity bill. These high values once again confirm that individuals are happy with the

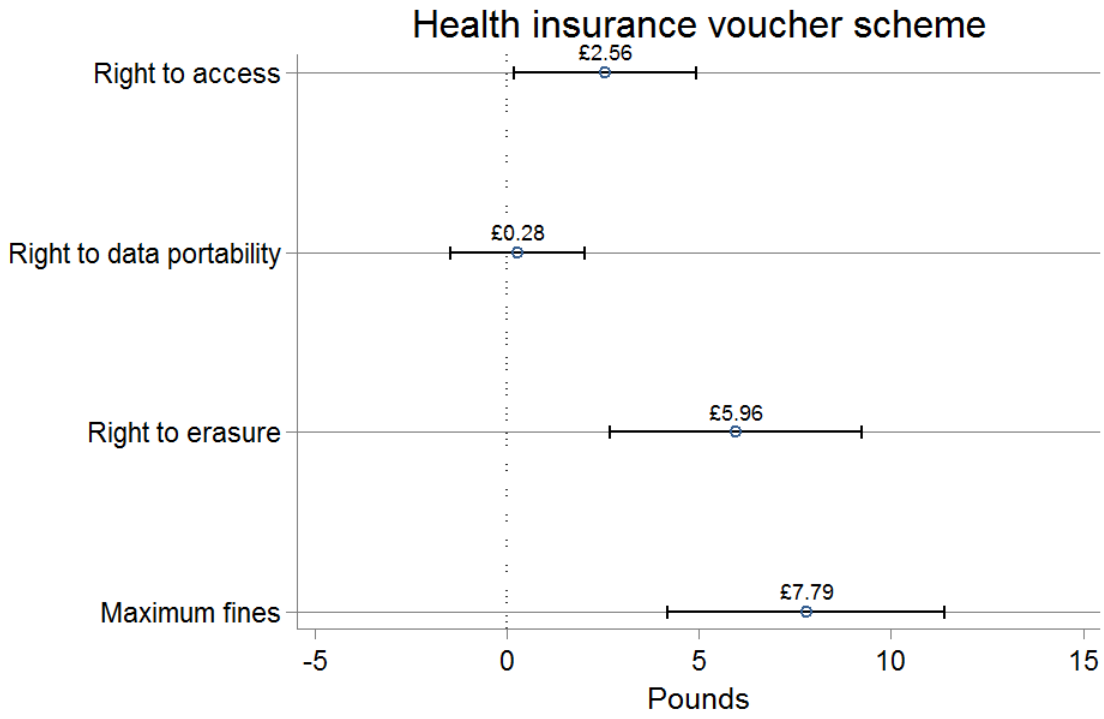
[20] This excludes the average consumer value for the right to data portability as this right has not shown to be important in the decision for smart meters; it is statistically insignificant.

package of rights they have, and that they need to be compensated significantly to give up their rights.

3.2.3 Health insurance voucher programme

The last context in which in which consumers made decisions was a voucher scheme run by a health insurance company. In this scheme, a health insurance company rewards healthy clients with vouchers giving discounts on goods and services such as clothes, cinemas and gyms, among other things. In return, participants need to provide personal data on their life style such as how far a participant walks, whether she goes to the gym or whether she goes for health check-ups.

Figure 15 Consumer valuation of GDRP rights: smart meters



Note: the bars around the central estimate show the 95% confidence interval.

Source: LE survey of consumers (2017) Choice experiment

Table 3 Average value to consumers of rights and fines, in the health insurance voucher scheme context

	Value in £	Value as percent of monthly spending on health insurance
Right to request complete details of the personal data the provider has on you	2.56	3%
Right to copy or transfer your personal data from the current provider to another	0.28	0%
Right to request the deletion or removal of personal data stored by the provider	5.96	6%
Provider faces a fine of £15m or 5% of turnover for non-compliance	7.79	8%

Note: The average total spending on health insurance used is £93, which is not derived from the survey.

Source: LE survey of consumers (2017) Choice experiment

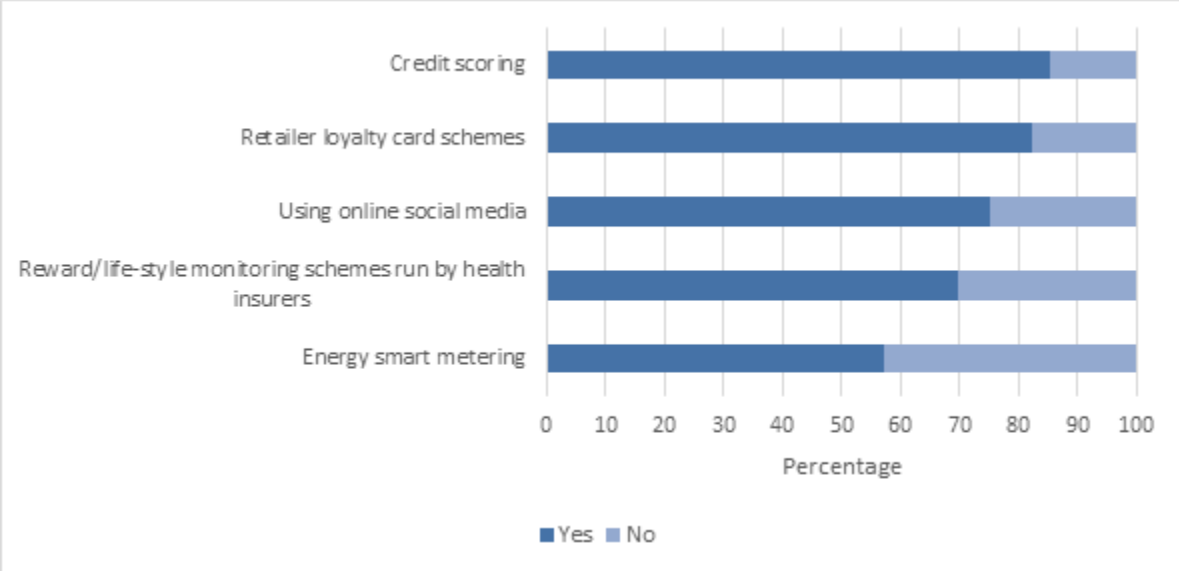
Table 3 shows the value of consumers for each of the rights, and the percentage of *monthly* spending on health insurance they represent. The average value ranges from £2.56 to £7.79, excluding the right to data portability, representing roughly 3 to 8 % of health insurance spending. The average savings are similar to the results found in the previous sections and confirm their findings.

3.3 Awareness & exercise of GDPR rights

The choice experiment shows that consumers are willing to forego savings equal to 5% to 10% to have the rights assigned to them in the GDPR. In the context of the choice experiment, the consumers were aware of their rights and could exercise them easily by making appropriate choices. This may not be true in a real world setting.

Consumers included in the choice experiment where asked whether they were aware that personal data is being collected as part of a number of common consumer transactions. Figure 16 shows the percentage of respondents that either are or are not aware of data collection in the three scenarios presented in the choice experiment, as well as social media and credit scoring.

Figure 16 Are you aware that your personal data is collected for:



Source: LE survey of consumers (2017)

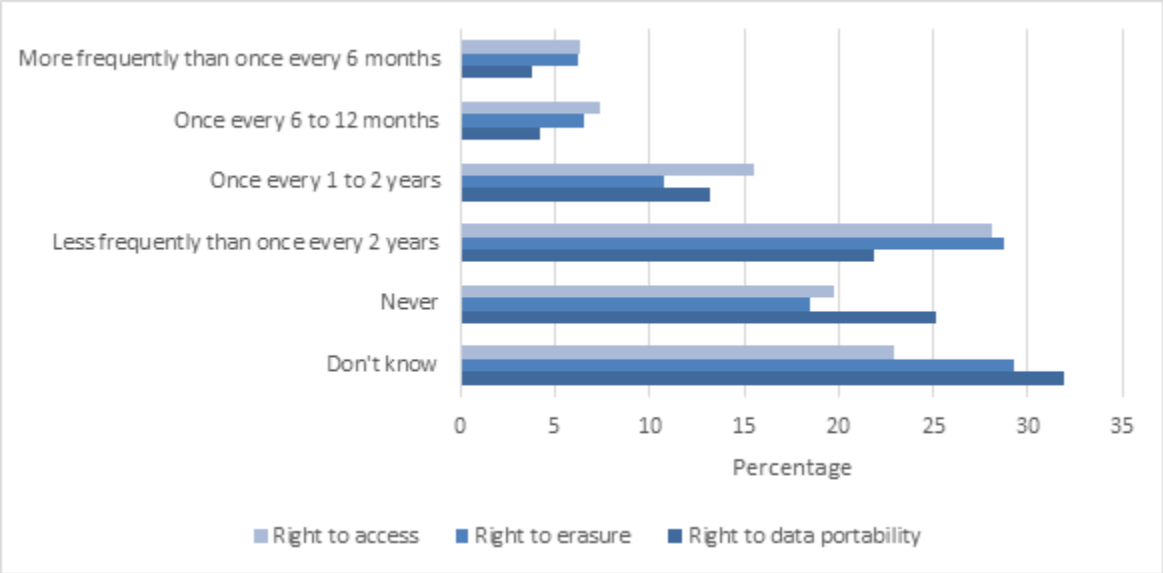
In all cases, the majority of consumers are aware of data being collected about them, but the spread varies. About 15% of respondents are aware of data collection by credit scoring agencies, which increases to 43% for smart metering.

Taken together, the evidence of the high valuation once data protection rights and trade-offs are made explicit and the evidence on limited awareness of data collection practices in different industries suggests that consumers value their rights even though they underestimate their scope (the areas in which data is collected), which implies they might underestimate the value of the rights.

The lack of awareness that data is collected has distributional effects: Taylor (2004) finds that if consumers do not anticipate firms' ability to use details about their past interactions for price discrimination their surplus is captured by firms.

Figure 17 shows that most people expect to exercise their rights infrequently at best. Given the lack of awareness of the right to data portability, it is not surprising that this right is likely to be invoked the least. Furthermore, many respondents note that they do not know how often they will exercise their rights.

Figure 17 How often do you think you would exercise your rights



Source: LE survey of consumers (2017)

The finding that consumers assign high values to their GDPR rights (they are willing to forego roughly 5% to 10% of savings on transactions that involve the transfer of personal data) together with the survey results that show a limited awareness of data collection that accompanies many common transactions and a low propensity to exercise the rights suggests that the benefits of GDPR do not depend directly on consumer engagement. At the same time, it is possible that increased awareness and increased exercise of rights would lead to higher benefits.

4 Professionals' views on benefits from GDPR rights

This section presents the evidence that has been collected on the specific benefits that can be expected to arise from individual GDPR rights. It is based on interviews with senior data professionals in large consumer-facing businesses in the UK, a series of online forums and an online survey of 250 data professionals. The primary evidence is supplemented by secondary sources, especially where these provide quantitative information on potential benefits. The purpose of the approach is to identify the benefits that are seen as likely to occur, and the likely economic impact of those benefits on businesses and consumers. The right of access, the right to erasure, the right to data portability and ancillary provisions (fines and DPOs) are discussed in turn.

4.1 Right of access

Box 3 Summary: Professionals' views on benefits from GDPR rights

The GDPR brings an incremental strengthening of the right of access.

Greater control for consumers over their data is seen by professionals as the most likely benefit, while more accurate data is seen as having the greatest potential impact on profitability for data controllers.

Access requests are interpreted by businesses as signals of consumer dissatisfaction. As such, they may incentivise good data protection practices.

There is a consistent discrepancy between the assessment of likelihood and the assessment of impact: The number of respondents that agree that a benefit impacts positively on profitability is consistently smaller than the number that see a benefit as likely.

A large proportion (typically the largest) is undecided on the question of benefits (neutral/neither agree or disagree), which signals a high degree of uncertainty, even among an audience (individuals with data protection responsibilities at their place of work) that can be expected to be more knowledgeable than the general population.

Finally, the pattern seen for the positive answers (more general agreement than expectation of commercial benefits) is reversed for the negative answers: a greater number of respondents strongly disagree that commercial benefits (increased profitability) will result from GDPR rights than see the existence of those benefits as extremely unlikely.

Definition of the right of access

Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed; access to their personal data; and other supplementary information. (ICO)

The right of access one's personal data exists under the current DPA, however, the right is strengthened by the GDPR (Article 15, 'right of access by the data subject') in several ways. Upon receiving an access request, personal data has to be provided to the subject:

- free of charge (unless the request is manifestly unfounded or excessive, e.g. repetitive);
- without delay and at the latest within one month of receipt; and
- in a commonly used electronic format.

Paragraph 2 of Article 15 further specifies that information needs to be provided on the safeguards in place if personal data is transferred to a third country or to an international organisation.

The changes brought about by the GDPR are marginal in that they do not expand the scope of the right as it currently exists. However, they lower the cost to consumers of exercising the right[21], thereby encouraging its use and presumably strengthening its effects.

Data professionals interviewed for this project stated unanimously that access requests (as well as erasure requests) are at present extremely rare. Two interviewees independently estimated that in their experience across various industries that less than one in a million customers currently make such requests[22]. Therefore, no appreciable effects of the right have been observed in practice[23].

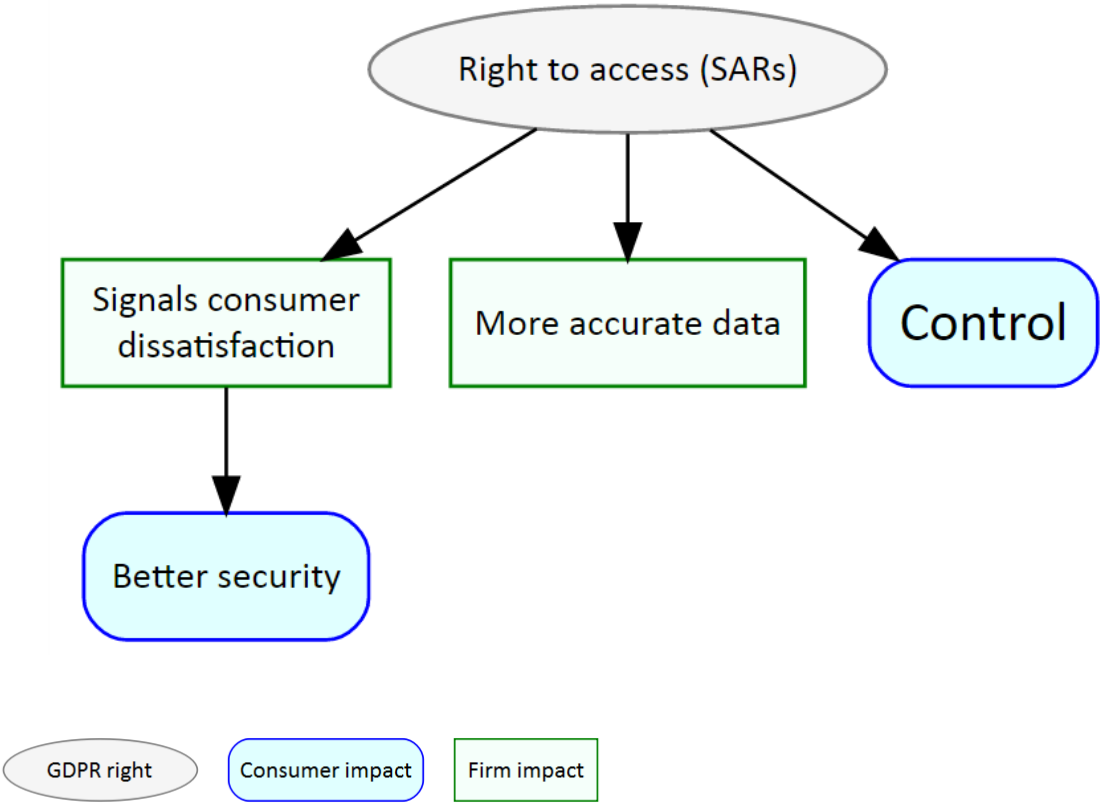
The following benefits were identified based on consultations and extrapolation from the text of the GDPR.

[21] Note that, according to an interviewee representing a high street retailer, in practice access requests are already typically processed free of charge by large organisations.

[22] However, it is possible that certain industries are affected by access requests to a much greater degree. The ICO received over 6,100 complaints about subject access last year.

[23] Respondents can envisage a short-term flare up in access requests after the GDPR comes into force in 2018. It was speculated that data journalists, data professionals and competitors would drive this, rather than individual consumers. In fact, the role of access requests as a tool to gather business intelligence could be seen as a source of benefit in its own right.

Figure 18 Benefits arising from the right of access



Note: A larger font size in the node indicates that more data professionals indicate that they think a benefit is likely or extremely likely to occur.
Source: LE

4.1.1 Professionals' view of benefits of the right of access

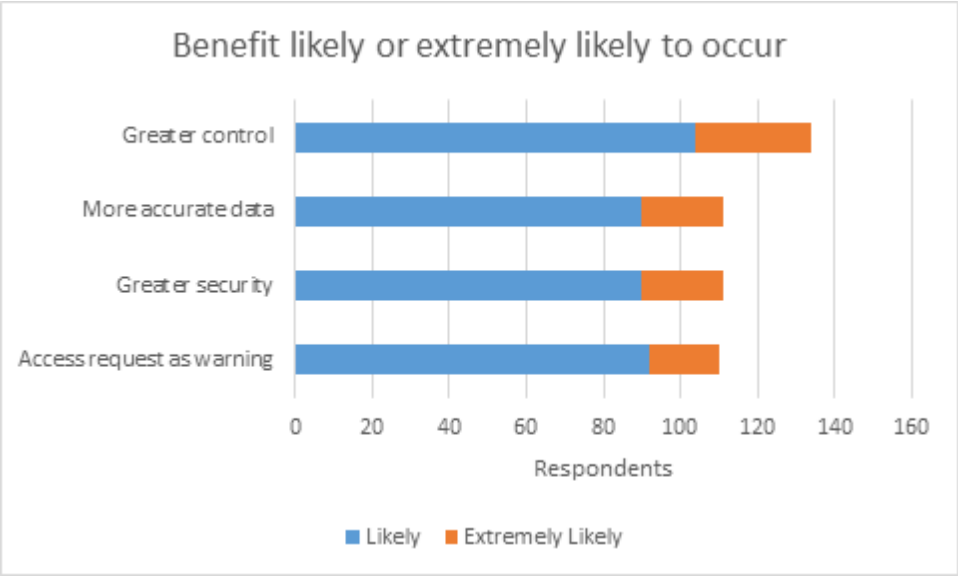
Data professionals were asked in an online survey to indicate:

- the likelihood with which benefits will occur; and
- the economic impact on their organisation.[24]

The results of the survey have been used to verify that the hypothesised benefits (Figure 18) are plausible and to rank the likelihood that they will occur from the perspective of data professionals. Detailed survey results are reported in Annex 3.

[24] Profitability was chosen as the most convenient (easily recalled) measure of economic benefit and a key contribution to gross value added.

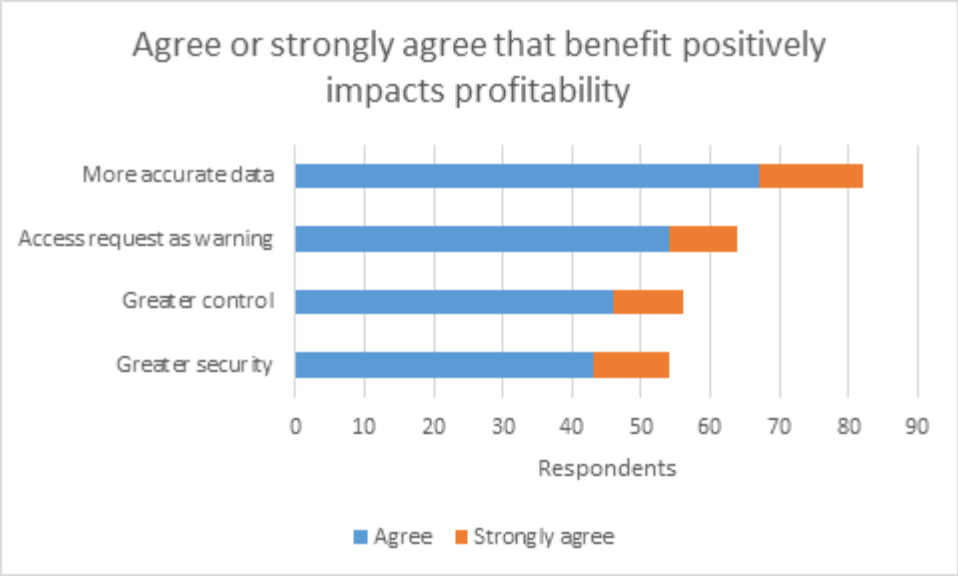
Figure 19 Likely benefits of the right of access



Source: LE survey of data protection professionals (2017)

A recurring finding is that many professionals consider benefits to be likely, but they are much less optimistic that commercial benefits will accrue to the organisations they work in. It is noticeable that survey respondents typically only see very direct benefits, such more accurate data, as leading to potential economic impacts on their organisations. With regard to greater control by individuals over their own personal data, while professionals recognise this as the most likely benefit, relatively few see this as a source of economic benefit for their organisations. Again this goes against the view that strengthening consumer confidence will have a direct incremental impact (see Section 2).

Figure 20 Impact of the right of access on profitability

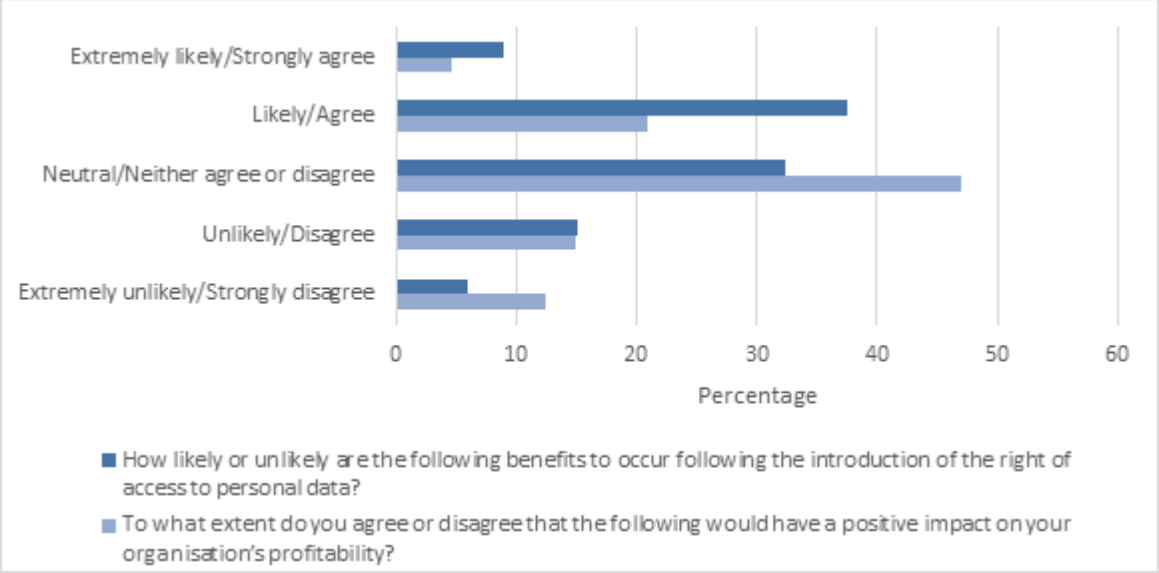


Source: LE survey of data protection professionals (2017)

Looking at the distribution of responses across all the potential benefits for the right of erasure (Figure 21), we see:

- A discrepancy between the assessment of likelihood and the assessment of impact: The number of respondents that agree that agree or strongly agree that a benefit impacts positively on profitability is consistently smaller than the number that see a benefit as likely or extremely likely.
- A large proportion (typically the largest) is undecided on the question of benefits (neutral/neither agree or disagree), which signals a high degree of uncertainty, even among an audience (individuals with data protection responsibilities at their place of work) that could be expected to be knowledgeable.
- Finally, the pattern seen for the positive answers (more general agreement than expectation of commercial benefits) is reversed for the negative answers: a greater number of respondents strongly disagree that commercial benefits (increased profitability) will result from GDPR rights than see the existence of those benefits as extremely unlikely.

Figure 21 Average response over all potential benefits



Source: LE survey of data protection professionals (2017)

The pattern of survey responses observed in relation to the right of access is repeated consistently for all the potential benefits across all rights that were investigated.

4.1.2 Access requests signal consumer dissatisfaction

The key mechanism through which the right of access one's personal data affects commercial relationships is as a **signal of consumer dissatisfaction**. Interviewees unanimously agreed that user access requests (which occur very infrequently under normal circumstances), would be seen as an indication that "something had gone wrong" in the customer relationship. However, respondents tend to see access requests in the context of a broader customer service dispute, not necessarily related to issues with personal data processing.

Interviewees also agreed that such a signal would be taken seriously and trigger action on the part of the data controller, and therefore was likely to lead to an objective improvement in security and processes more generally.

Several business representatives were concerned that new business models might spring up that use access requests (potentially coupled with the threat of erasure) to exert pressure on companies in the wake of a data breach, akin to firms touting for custom for speculative claims in relation to mis-sold payment protection insurance (PPI). Such 'fishing exhibitions' could be highly damaging for a firm's reputation, and there may be direct harm from by follow-on claims against a company that is being fined by the ICO.

4.1.3 Other benefits

A strengthened right of access enhances user control over their personal data. However, the effect is expected to be small. One interviewee recounted that attempts by various service providers to add value to their online offering by providing consumers with data access and tools to interrogate their usage patterns (e.g. for current accounts) have failed and were discontinued due to a lack of demand.

However, one interviewee, head of customer analytics and modelling for a high street retailer, observed that giving people access to their data could be used in innovative ways by companies. Providing a platform (website) through which customers can access and inspect the personal data that is being held on them could become a tool for improving data quality (allowing users to correct wrong information), elicit additional information, set permissions and opt in to marketing. However, whether this realistic is uncertain, as the investment in the relevant software and infrastructure (data needs to be available instantly and highly processed to be accessible to users) might not be justified when data volumes are large and consumer interest is low.

Data professionals interviewed for this study agreed that businesses have a lot to gain from more engaged customers (for example by getting access to more accurate data, if consumers do not resort to 'informational self-defence' by providing wrong data).

Overall, while more accurate data was seen as highly valuable (and inaccurate/obsolete data seen as an acute problem), the role of access requests was seen as purely hypothetical in this context.

While it is plausible that the requirement for transparency about international data transfers will incentivise security in relation to such transfers (or even a revision of transfer policies), this effect must be considered negligible on based on present evidence.

4.2 Right to erasure

Box 4 Summary: Right to erasure

The right to erasure is a substantial change compared with the current legislation.

The right to erasure is seen as an extension or further strengthening of the right of access.

The most likely benefits arising directly from the right to erasure are the end of harmful use of data and greater control of consumers over their data.

The right to erasure reflects consumer preferences and is seen as important in the decision to give out information.

Like access requests, requests to erase personal data are also seen as evidence of consumer dissatisfaction.

There is little expectation that the right to erasure will be exercised often, driven partly by a lack of consumer awareness.

Definition of the right to erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, e.g. where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; when the individual withdraws consent; or when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing. (ICO)

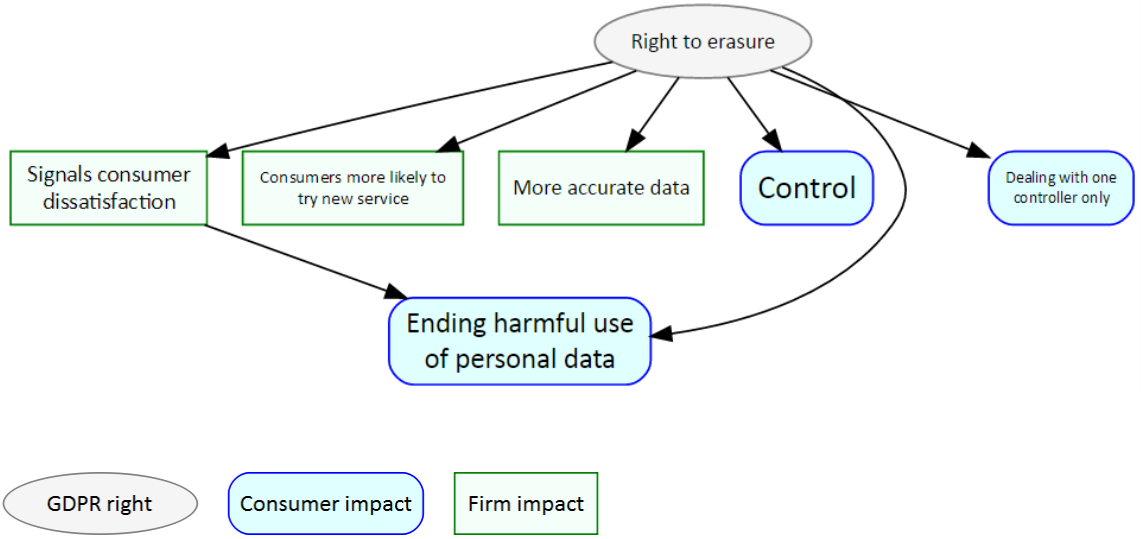
The right to erasure (Article 17) is a substantial change compared with the DPA. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress.

Theoretically, the right to erasure has potentially conflicting impacts. At a high level, "society may suffer when certain behaviors stay hidden (consider insider trading or social progress being delayed and social norms failing to evolve because of individuals' fears of disclosing legitimate but fringe opinions); but society may also benefit when other information is suppressed (around the world, various jurisdictions allow certain juvenile criminal records to be expunged with the belief that unfettered reintegration of minors has positive social value)."[25]

The benefits of the right to erasure (Figure 22) are related to the right of access discussed above. The right of access can be seen as enabling the right to erasure, and the threat of erasure arguably contributes to the benefits of access (the threat of erasure hangs over any access request, and the feeling of control is strengthened by the knowledge that users not only know what is kept about them, but that they can take action if they want to).

[25] Acquisti et a. (2016), p. 446

Figure 22 Benefits arising from the right to erasure



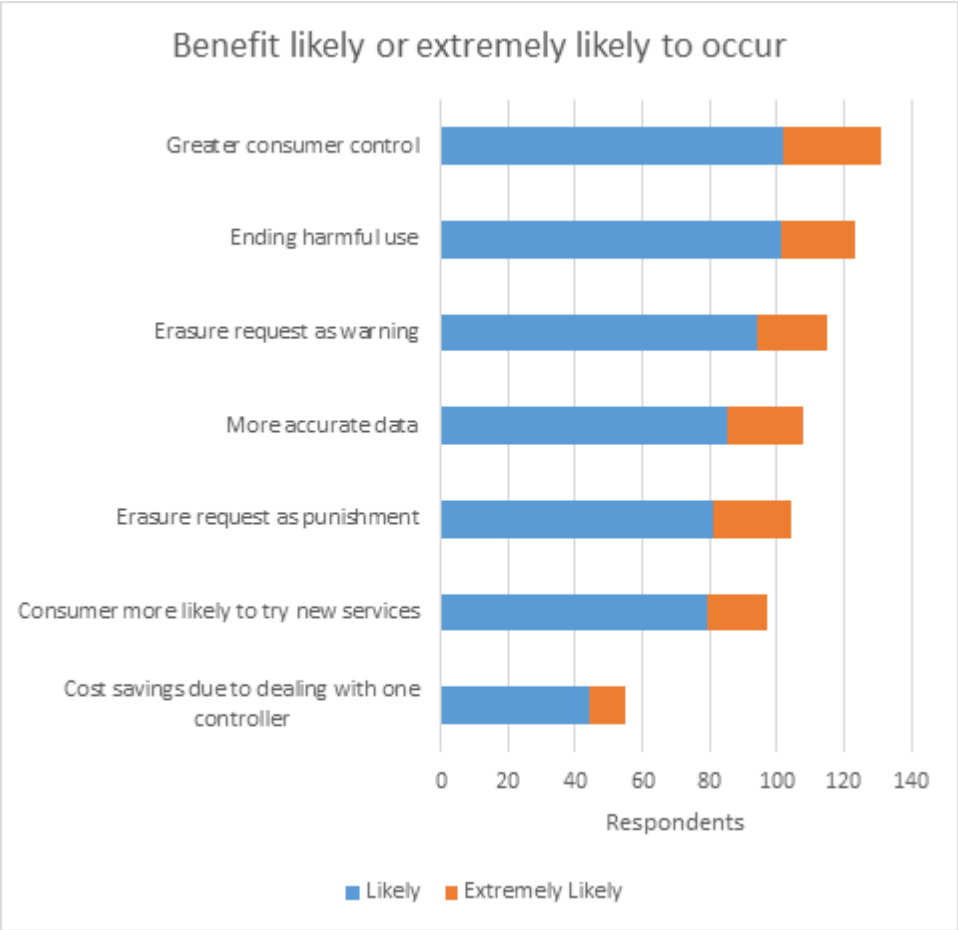
Note: A larger font size in the node indicates that more data professionals indicate that they think a benefit is likely or extremely likely to occur. Minimum font size has been set to 8 points for readability.
Source: LE

4.2.1 Professionals' view of benefits of the right to erasure

The online survey of professionals asked whether the benefits in Figure 22 will occur and to which extent these will benefit their firm.

In terms of likelihood of occurring, three potential benefits stand out; two positive and one negative. Data professionals are most optimistic about the GDPR leading to reduced harmful use of personal data and more control of consumers. At the same time, they seem most pessimistic about the idea that the right to erasure leads to cost savings on the side of the consumer because they only need to deal with one data controller to get their data erased.

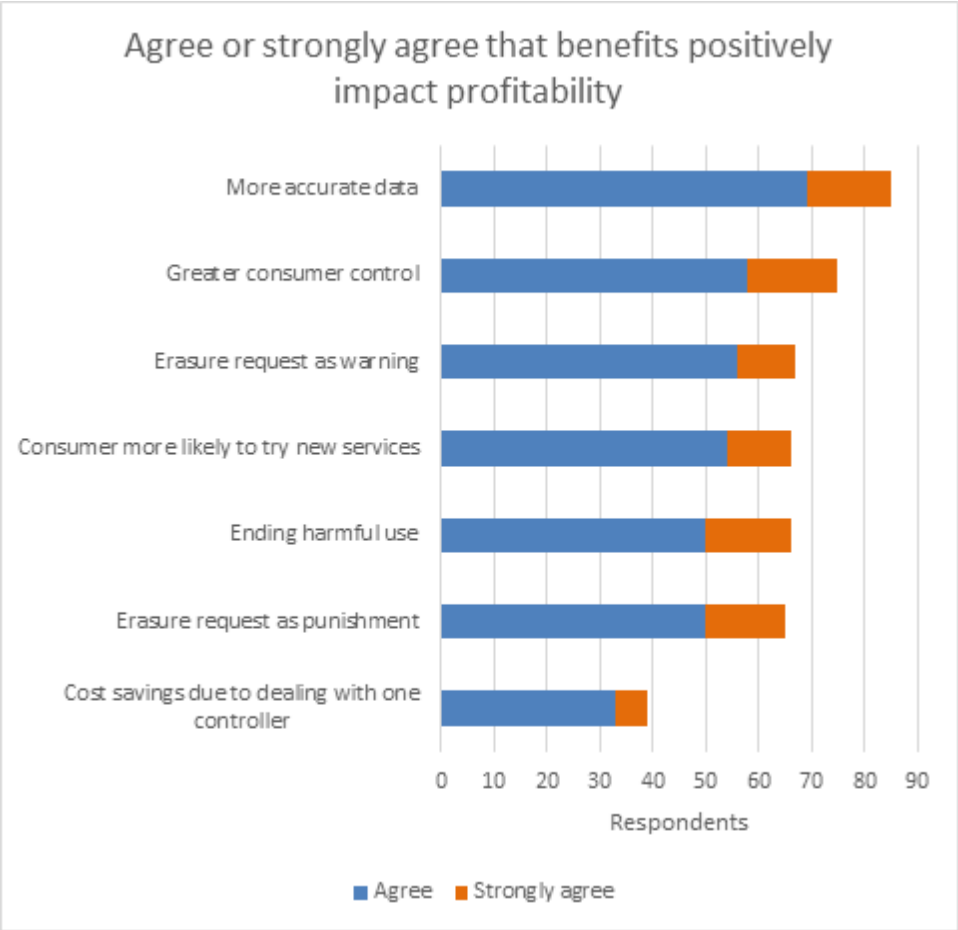
Figure 23 Likely benefits of the right to erasure



Source: LE survey of data protection professionals (2017)

As before, professionals see a potential positive impact from more accurate data on their organisations' profitability, but they see this as less likely to occur than other benefits.

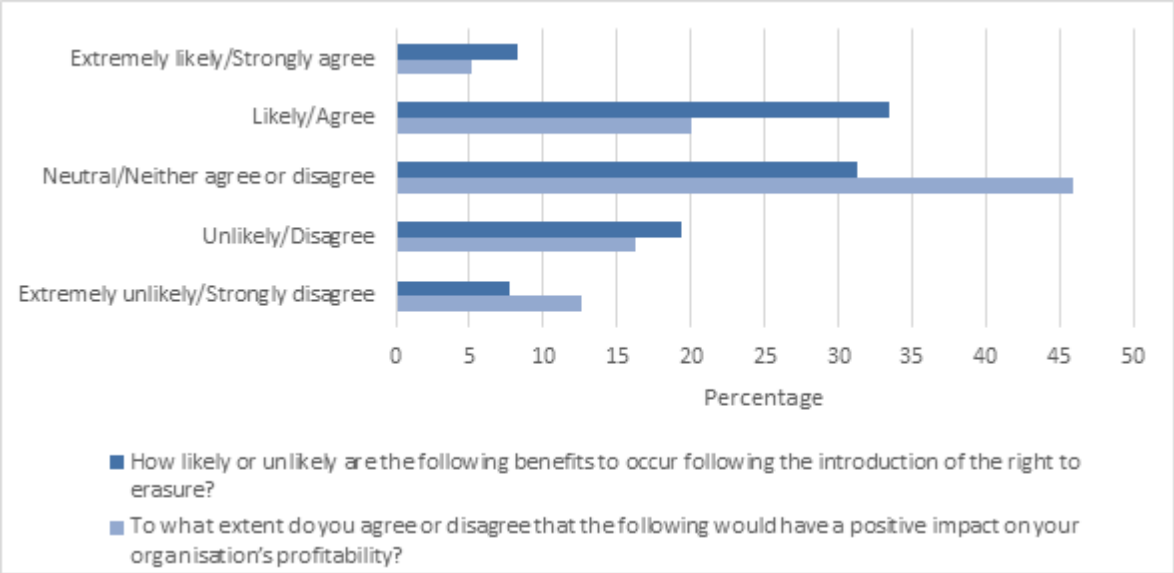
Figure 24 Impact of the right to erasure on profitability



Source: LE survey of data protection professionals (2017)

As with the right of access, the most frequently chosen option is "neutral" or "neither agree or disagree". This, once again, highlights the difficulty to provide predictions on the benefits arising from improved personal data rights.

Figure 25 Average response over all potential benefits



Source: LE survey of data protection professionals (2017)

As seen for the right of access, data professionals are more pessimistic about the impact of the on their organisations. Again, almost universally, respondents believe that positive impact on their organisation are less likely than a benefit occurring in the future, as highlighted by the average responses.

4.2.2 Erasure requests signal consumer dissatisfaction

Like access requests, but more so, erasure requests signal consumer dissatisfaction. Business representatives said they would be highly concerned if they received erasure requests, and would see them as evidence that the customer relationship had broken down:

"The truth is people know they have to swap their data for all kinds of goods and services and most will never be bothered to exercise their new found 'right to be forgotten' unless they become stupidly angry with a company." **Cave (03 February 2017)**

"If people started requesting erasure, we'd feel like we had failed".

"In my experience customers are more sensitive to the risks of data security than they are to the rights of access or erasure; however if there were to be any security or other breaches, the way we react to access and erasure requests would become critical to protect the company's reputation as a responsible holder of information" **LE online forum (2017) Head of Data, B2B Operations**

However, erasure requests occur very seldom at the moment. Unlike in the case of access requests, the GDPR does not lower the cost of requesting erasure[26], but instead increases the scope of the right, so an increase in

[26] With the exception of Paragraph 2, which instates a sort of one-stop-shop if the personal data is processed by multiple controllers. However, the reach of this provision is very uncertain, as it relates only to personal data that 'made public' by the controller.

erasure requests can be expected only if it is mediated through more frequent access requests, which are then followed by erasure requests[27].

Erasure requests are expected to be more likely following incidents that undermine consumer trust (data breaches etc.). The threat of large-scale erasure requests represents a strong incentive for data security. As discussed in relation to access request, it can be imagined that third-party services will emerge to bundle consumer pressure on providers, which would amplify the incentive still further.

4.2.3 Ending harmful use of personal data

An obvious result of erasure is that any harmful use of one's personal data is discontinued. Again it should be considered that this benefit is not uniquely dependent on the GDPR (rules on direct marketing, nuisance calls etc. already exist).

However, there is strong evidence that unsolicited online communication ("spam") causes considerable harm. For example, Ferris Research (2009) estimate that spam cost $130 billion worldwide in lost productivity.[28] Erasure could also be used as a defence against price discrimination[29] and put a stop to escalating efforts by direct marketers to counteract the use of technologies that prevent unsolicited marketing[30]

Ofcom has done research into the harm caused by silent/abandoned calls[31]. In it, it has provided some calculations of the costs of such calls. This data can serve as an analogy for the benefit of ending other forms of unwanted contact that arises from firms' access to personal data.

Ofcom has used two ways of estimating the cost of nuisance calls. The first is a time cost approach, i.e. adding up the cost of the time spent answering unwanted calls into an annual figure. Calculations for these are in the next figure:

[27] Some of the forum participants stressed that they would be concerned only if requests came in frequently. A single erasure request is generally not seen as a signal of consumer dissatisfaction.

[28] Other researchers have found lower, but still very substantial costs, e.g. Rao and Reiley (2012), who estimate an overall societal cost of spam of $20 billion.

[29] Villas-Boas (2004)

[30] Hann et al. (2008)

[31] https://www.ofcom.org.uk/__data/assets/pdf_file/0015/80700/annexes_7-8.pdf

Table A7.2 Time cost approach calculation

	Value of time (£ph)	Time per call (secs)	Cost per call (£)	Volume of potentially harmful calls (p.a.)	Harm estimates (£m p.a)
Silent calls	7	27	0.05	1,423	76
	12		0.09		126
	16		0.12		177
Abandoned calls	7	28	0.05	172	9
	12		0.09		16
	16		0.13		22

Note: The volumes of calls recorded here removes those marked as 'not a problem' or 'useful' and hence do not match those in Table A7.1.

Source: Ofcom calculations based on Ofcom and GfK (2015), 'Landline nuisance calls panel research Wave 3 (January – February 2015)'.

The second is a willingness to pay exercise to avoid nuisance calls. Again, this cost would be considered a benefit if avoided. Results in the table below:

Table A7.4 Proportion of call types received on landline

Willingness to pay per month	Proportion	Affected population (m)	Harm per month (m)	Harm per year (m)
£0.00	69%	36	0	0
£0.50	17%	9	4	53
£2.00	8%	4	8	101
£5.00	4%	2	10	126
£10.00	2%	1	10	126
Total	100%	52	34	406

ONS mid-year 2014 population estimate of 57m UK adults aged 16+ and an Ofcom market monitoring estimate of 84% of adults having a landline.
Source: Ofcom calculations.

An interesting point in relation to potentially unwelcome advertising messages targeted at consumers was raised by one interviewee: online ads are targeted in a variety of ways, not all of which rely on personal data held by the advertiser. This means that consumers may still see targeted ads from businesses they had previously asked to erase their data. This illustrates the fact that many aspects of digital markets that impact consumers and businesses are not related to personal data and therefore not directly affected by the GDPR.

4.2.4 Cost savings from having to deal with only one data controller

Paragraph 2 of Article 17 stipulates that where a controller has made personal data public, he "shall take reasonable steps (…) to inform controllers which are processing the personal data that the data subject has requested the erasure". The circumstances under which this right applies and is relevant for commercial transactions are somewhat uncertain. However, it is clear that the consumers will find it easier to erase their data from multiple controllers' databases *under certain circumstances.*

4.2.5 Option value: consumers more likely to try data intensive services

"The willingness to participate in tests is really a question of relevance to the individual in question. Whilst interest drives the decision, the "right to be forgotten" is another good reason to go ahead. It may sway those who are "undecided" and convince them to take the plunge." **LE Forum (2017) COO and compliance assistance, finance**

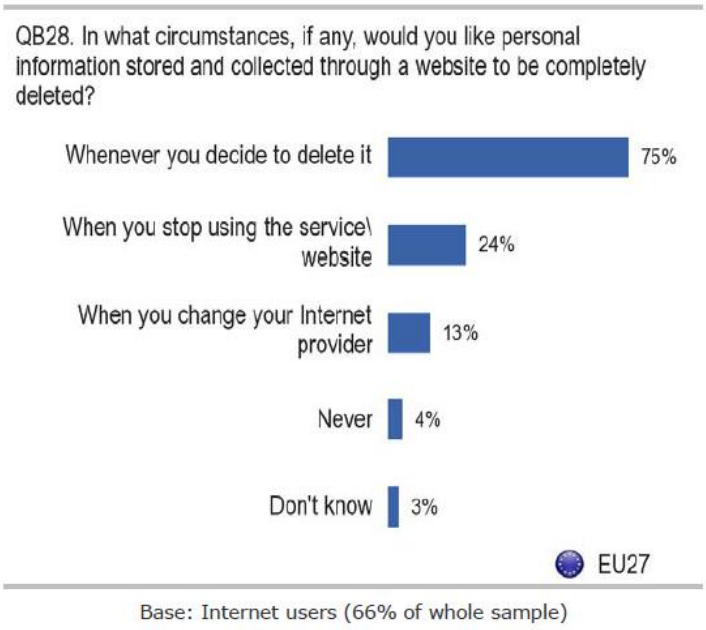
Another benefit may be that the right to erasure increases the willingness of consumers to test new services, knowing that their data can be erased if the service is not to their liking. Most forum participants do not to believe this logic, with only two positive responses to the idea.

Some forum participants note that the rights to erasure will not lead people to attempt new services directly, but it may tip the balance for those undecided. One respondent noted that the rights may not lead to more consumer providing data, but that it may lead to a given consumer giving more data.

4.2.6 Control

A more comprehensive right to erasure is in line with reported consumer preferences (Figure 26) and can thus be expected to contribute positively to consumer confidence in transaction that involve disclosure of personal data.

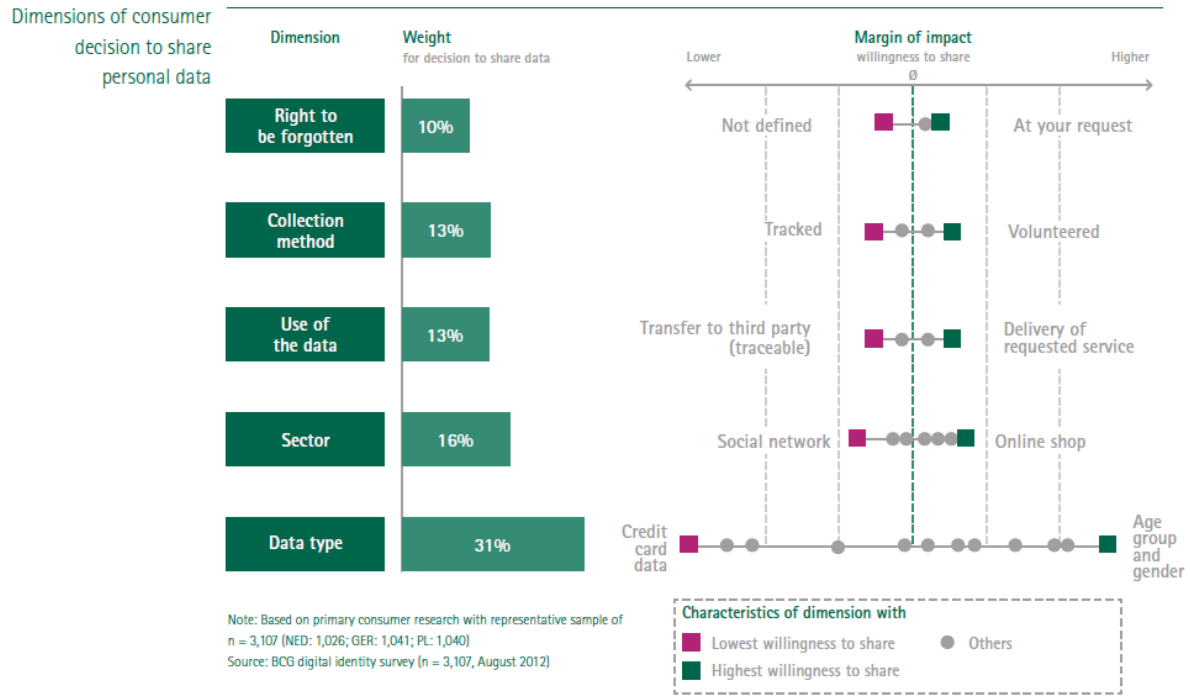
Figure 26 Consumer views on the scope of the right to erasure



Source: Special Eurobarometer 359 (2010)

Based on survey evidence, there is support for the hypothesis the right to be forgotten has an appreciable impact on individuals' willingness to share data (Figure 27).

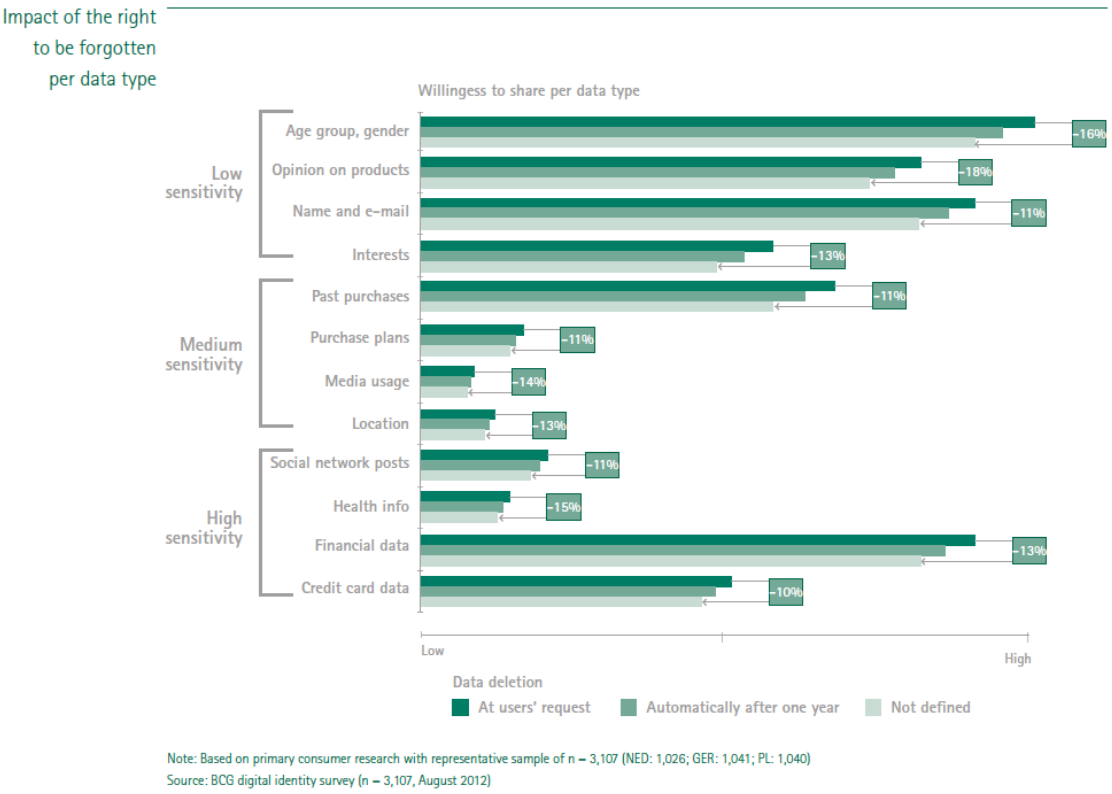
Figure 27 Dimensions of the consumer decision to share data



Source: Boston Consulting Group (2012) – The value of our digital identity

BCG (2012) found that erasure on request increases willingness to share data consistently for all data types.

Figure 28 Impact of the right to be forgotten



Source: Boston Consulting Group (2012) – The value of our digital identity

Forum participants largely think that the rights indeed do create confidence, although some also note that this is dependent on the circumstances of the specific firm. Some respondents note that the right of access and erasure may not be the most important factors for trust, but that they become crucial in case of data breaches, for instance to protect brand reputation.

4.2.7 More accurate data

Erasing personal data by individuals who do not want their data being held/used in a certain setting can improve the quality of the dataset overall. This is a potentially important benefit for business, as "poor quality customer data is costing UK organisations 6% of revenue every year.[32]" Another immediate benefit of erasing records can be that wasteful spending on marketing is reduced.

Most forum participants agree that inconsistent data is a big problem and that consistent data is important to the firm. Whether the rights to access and erasure will improve consistency is less clear from the responses. Some participants note that the rights should improve consistency, but that it ultimately depends on whether consumer will exercise their rights.

[32] (New Customer Data Research Report 2017, Royal Mail Group in conjunction with DataIQ, http://www.dataiq.co.uk/land/6-solution-how-customer-data-drives-marketing-business-performance).

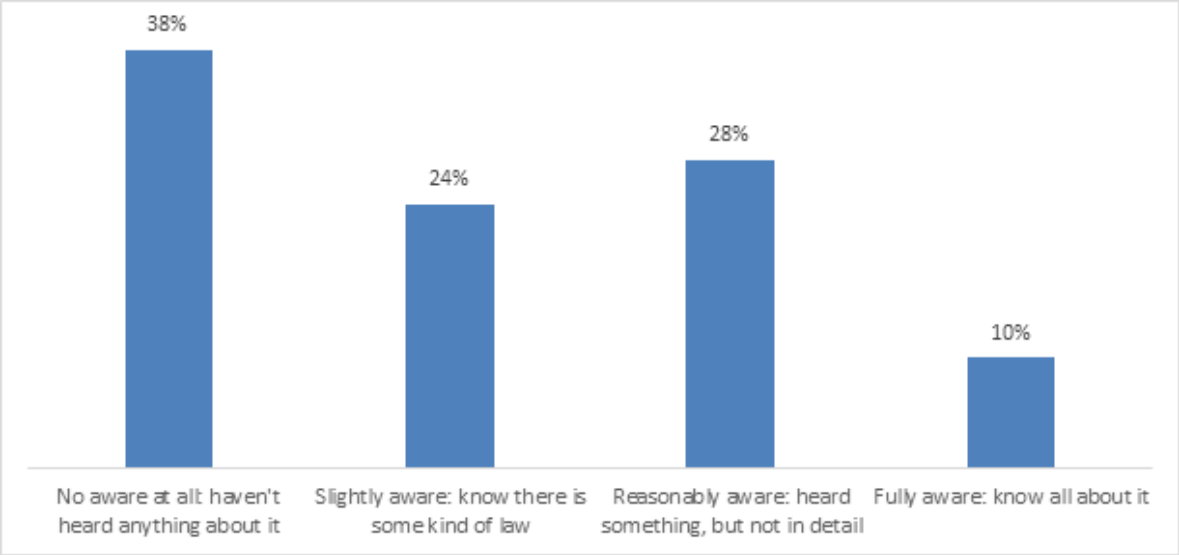
One participant, answering negatively to the question whether the rights to access and erasure will improve data consistency, noted that there are many sources of inconsistencies that these rights do not address.

"Assuming enough customers exercise that right then I would expect the consistency of data held to improve" **LE forum (2017) Head of Data, B2B Operations**

However, depending on the type of analytics that is applied to the dataset, a dataset from which observations are erased may lose value compared with the same dataset in which the records are still present, but de-activated for marketing purposes: a record that is no longer needed for marketing (because the consumer has opted out), can still be valuable, for example for analysing what determines customer attrition, for training algorithms and improving predictions/classification processes and thereby help producing better outcomes for existing customers.

Overall, it seems that the rights to access and erasure may benefit the consumer by fostering confidence, but this effect is reduced by the lack of awareness by consumers that they have the rights. This mimics the findings for data portability, which also finds some potential consumer benefits but these benefits are reduced by awareness. The figure below presents recent (2017) survey evidence on the widespread ignorance of data protection law among UK consumers. The survey carried out for this study finds relatively high levels of awareness (up to 68% for the right of access one's personal data, see Figure 9, p. 13). However, self-reported awareness levels are likely to overstate the true picture, as people claiming awareness may still be wrong in their understanding[33].

Figure 29 Consumer awareness of data protection law



Source: DataIQ (2017), Figure 1.2, p. 7

On the side of the firms, the rights to access and erasure may lead to more adventurous consumers – more willing to try new, data intensive services – which in turn may lead to higher profits. Furthermore, the rights may lead to more consistent data, and the right to erasure particularly may

[33] See LE (2012).

serve as a signal of consumer dissatisfaction which can be acted upon. It seems that there are multiple avenues from which firms may derive benefits to the rights to access and erasure.

4.3 Right to data portability

Box 5 Summary: Right to data portability

The right to data portability is potentially the most far-reaching change from current legislation, and has the largest expected impact on the relation between data controller and consumer.

An increase in competition in markets that rely on the use of personal data is potentially the greatest source of benefit, but this does not come out strongly in the survey evidence. Uncertainty about the scope of the right and the new business models that may be enabled by the right make an assessment difficult.

Consumer switching – which data portability would enable – has been shown to be beneficial.

Time savings and the existence of markets for secondary data are seen as the benefits most likely to arise.

Greater consumer control is seen as a less likely benefit of the right to data portability.

Definition of the right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them[34] *to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.* (ICO)

The right to data portability as defined by the GDPR (Article 20) is perhaps the most momentous change in terms of its impact on the relationship between individuals and businesses that store and process personal data. The aim of the right to data portability is twofold:

- First to empower data subjects regarding their own personal data.
- Secondly to encourage and facilitate innovation in data uses and to promote new business models linked to more data sharing under the data subjects' control.

[34] The right to data portability consists of two parts, "the right to receive" and "the right to transmit" (Art. 20(1)): data subjects can either receive their personal data directly and pass it on themselves or, "where technically feasible" (Art. 20(2)), they can direct a data controller to port their personal data to another controller.

The scope of the right to data portability is wide, although the full extent of its reach is as yet not understood. The crucial question of data formats, for example, is not addressed exhaustively in the legislation[35].

However, it is clear that he right applies "not only to personal data actively and knowingly provided by the data subject but also to pseudonymised data that can be clearly linked to a data subject and to personal data generated as a result of user's activities (such as search history, traffic data, location data or raw data generated by a smart meter or fitness tracker)"[36]. The right also appears to encompass any relevant metadata, so as to "preserve the precise meaning of exchanged information"[37].

Of the new GDPR rights, data portability has the most obvious and immediate impact on commercial relationships. It is also the only GDPR right that is cited by the EC as a source of direct benefits for business. Data portability is seen as enabling competition, as the quote from the EC's factsheet "What benefits for businesses in Europe?" in Box 6 shows[38].

Box 6 Example of business benefit (EC, 2016a)

"A new small company wishes to enter the market offering an online social media sharing website. The market already has big players with a large market share. Under the current rules, each new customer will have to consider starting over again with the personal data they wish to provide to be established on the new website. This can be a disincentive for some people considering switching to the new business.

WITH THE DATA PROTECTION REFORM:

The right to data portability will make it easier for potential customers to transfer their personal data between service providers. This promotes competition and encourages new businesses in the marketplace."

Source: European Commission Directorate-General for Justice and Consumers (2016). Data Protection Reform Factsheet "What benefits for businesses in Europe?" Retrieved from http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404.

Survey evidence also indicates that consumers see portability as important (Figure 30).

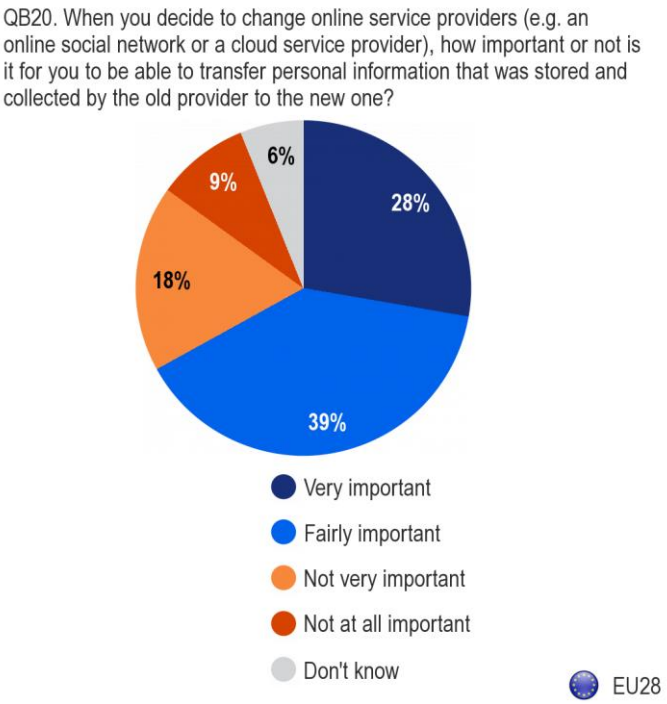
[35] The GDPR provides general guidance on what is expected at Art 20 and recital 68: "structured, commonly-used, machine-readable format" with recital 68 adding "interoperable". The Article 29 Working Party Guidelines state: "Given the wide range of potential data types that could be processed by a data controller, the GDPR does not impose specific recommendations on the format of the personal data to be provided. The most appropriate format will differ across sectors and adequate formats may already exist, and should always be chosen to achieve the purpose of being interpretable and affording the data subject with a large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach." The Article 29 Working Party recommends that industry stakeholders and trade associations "work together on a common set of interoperable standards and formats" that would facilitate this; however, "Where no formats are in common use for a given industry or given context, data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction."

[36] Ustaran and Choi, 16 December 2016

[37] Ibid. The provision of "suitable metadata" is a recommendation of the WP29 guidelines, p. 18.

[38] Note that portability thus my play an important role in balancing the overall effects of GDPR: Campbell et al. (2015) show that consumers are more likely to grant opt-in consent to large networks with a broad scope, rather than to less established firms. Portability counteracts this undesirable consequence.

Figure 30 Importance of data portability



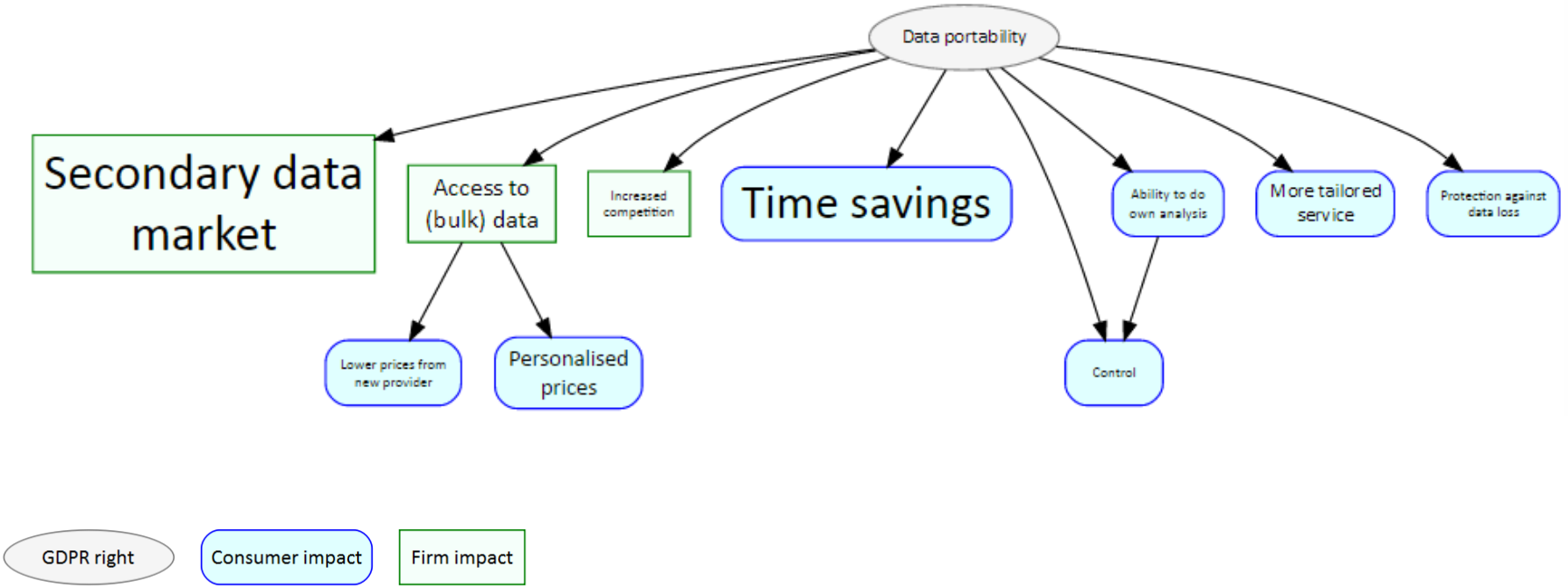
Source: Special Eurobarometer 431 (2015)

However, views on how important the right is going to be in practice are very mixed. Most of the individuals consulted see a great potential impact driven by new business models, rather than changes in the behaviour of individuals[39].

The benefits of data portability are varied. A summary is provided in Figure 31.

[39] Participants in the online forum unanimously agreed that they do not expect consumer to exercise the right to data portability in the near future, and neither do they expect to consumers to switch to or from competitors.

Figure 31 Benefits arising from the right to data portability



Note: A larger font size in the node indicates that more data professionals indicate that they think a benefit is likely or extremely likely to occur. Minimum font size has been set to 8 points for readability.
Source: LE

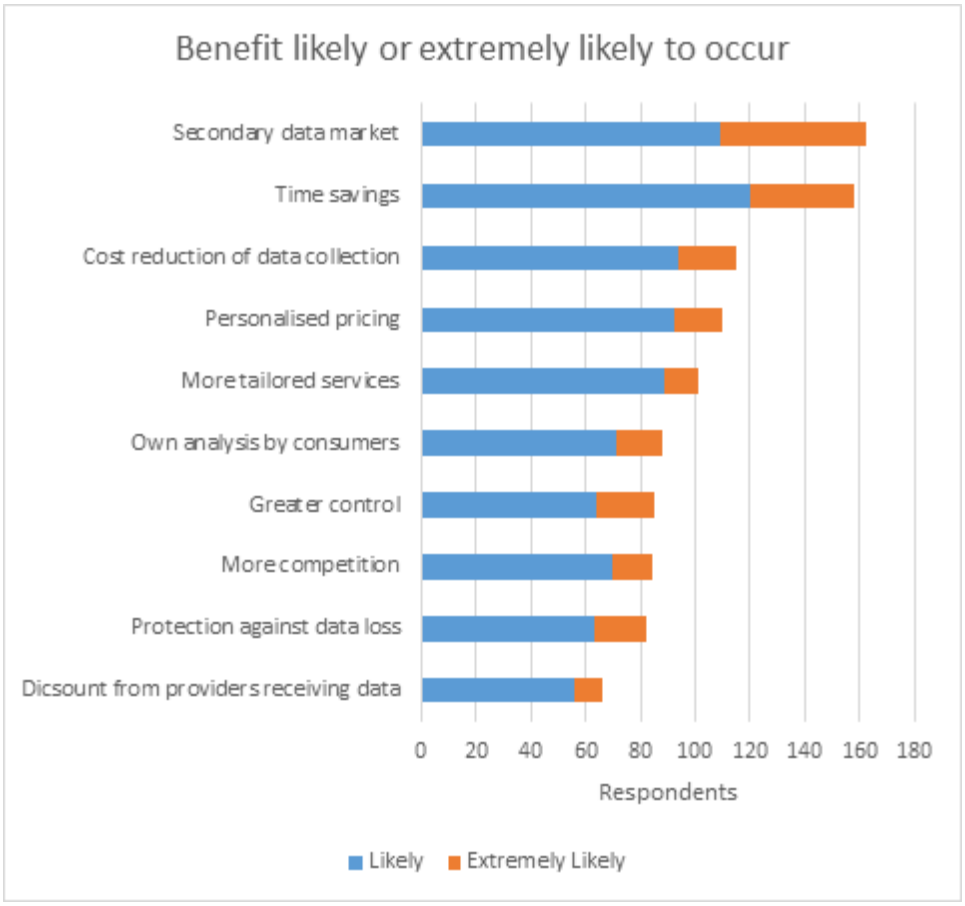
4.3.1 Professionals' view of benefits of the right to data portability

The respondents were asked to gauge the extent that the benefits hypothesised in Figure 31 will occur with the introduction of the GDPR and to which extent these will impact their organisation. The results are presented in Figure 32 and Figure 33.

The responses allow to gauge which benefits more likely to occur. Time savings and the creation of a secondary market for data stand out as the two benefits which are most likely to occur according to the survey respondents.

The benefits of a secondary market for data are potentially very substantial, but a lot of uncertainty exists about the magnitude of the benefits and how they will occur. This is unsurprising, as the benefits are likely to arise from new business models and greater use of newly mobile data across the economy. This uncertainty makes the benefit inherently difficult to quantify. However, research in this area suggests very significant impacts. For example, a 2014 study by Ctrl-Shift finds that a mature market for Personal Information Management Services (which would be enabled by data portability) could be worth £16.5 billion, 1.2% of UK GDP.

Figure 32 Likely benefits of the right to data portability

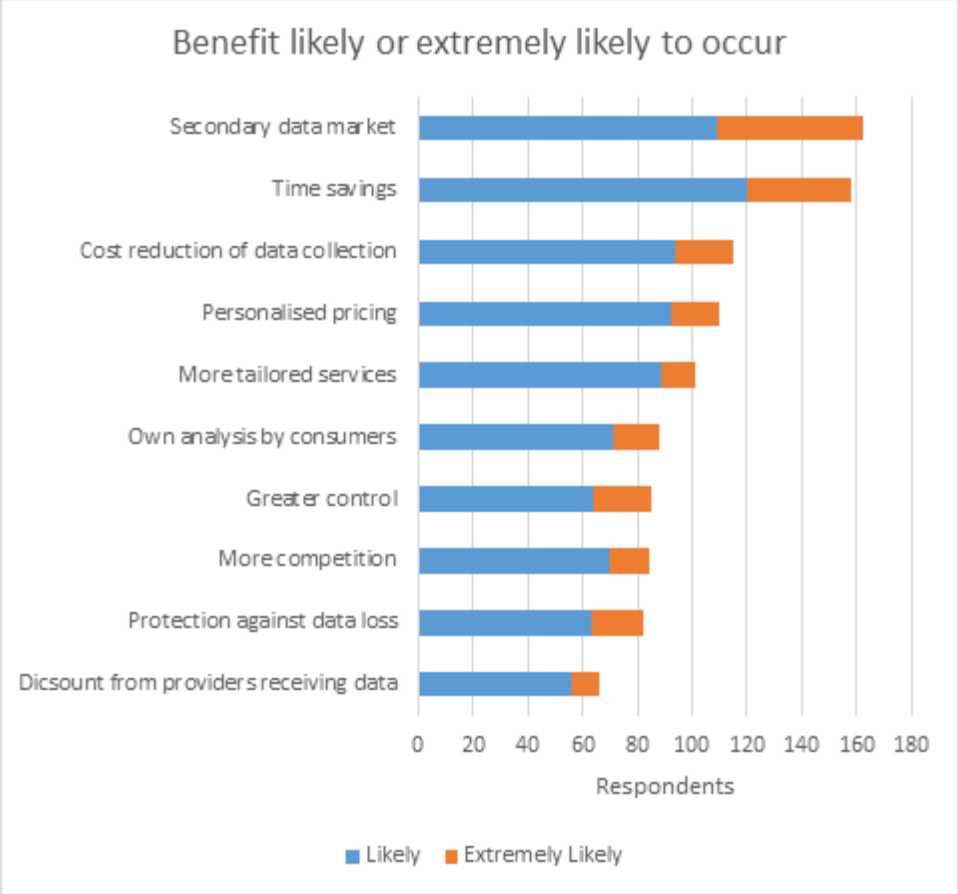


Source: LE survey of data protection professionals (2017)

The responses to whether benefits will impact the firm positively follow the pattern described previously for the other rights. Professionals expect benefits from data portability, although there

is less certainly about whether these benefits will result in increased profits for their own organisation.

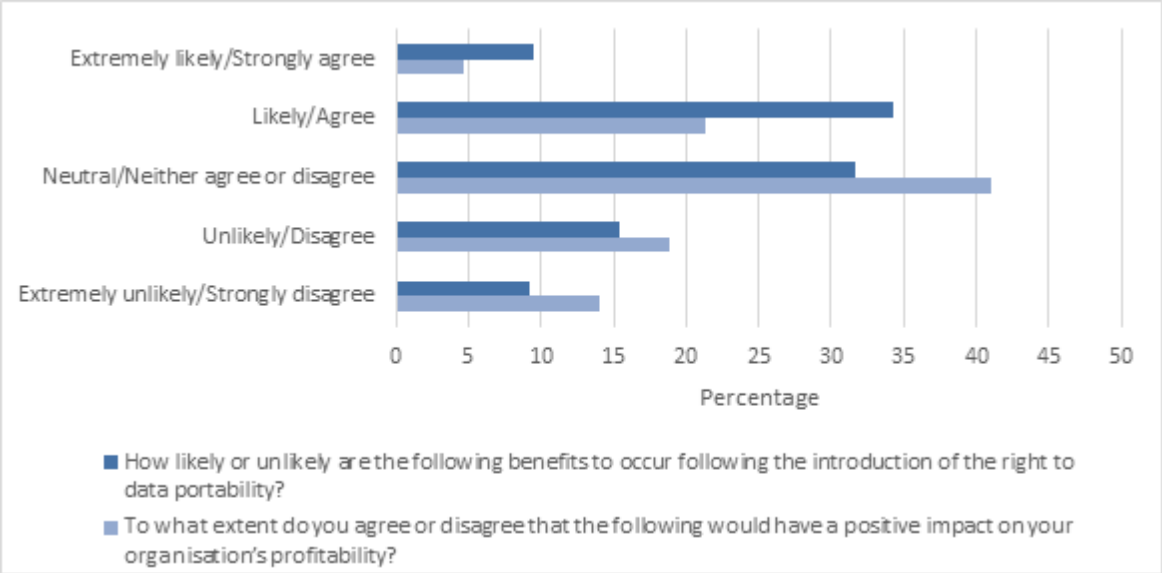
Figure 33 Impact of the right to data portability on profitability



Source: LE survey of data protection professionals (2017)

As before, data professionals find it difficult to establish whether benefits from the GDPR will arise and whether it will benefit their firm, with "neutral" or "neither agree or disagree" being the most popular choice for most potential benefits.

Figure 34 Average response of all potential benefits



Source: LE survey of data protection professionals (2017)

Even taking into account the apparent difficulty in assessing benefits, the responses are more optimistic than pessimistic. On average, the professionals are most likely to agree that benefits will occur.

4.3.2 Time savings (less time spent on entering information)

Time savings that arise when a data subject requests a controller to port his or her data to another controller are perceived as a real benefit by consumers. An indication of the importance of this aspect of data portability is given by a 2015 Eurobarometer survey, which found that time savings were cited by 12% of respondents as a reason why they disclosed personal data in online transactions.

Figure 35 Evidence of time savings as a rational for disclosing personal data

Source: Special Eurobarometer 431 (2015)

"It does not take users very long to input their data - a matter of moments. Consequently the time that portability would cut would be negligible. (…) I doubt many people will be aware of or understand the significance of the right so the opportunities it will present will be very limited." **LE online forum (2017) Data protection professional, retail**

However, participants in our online forum unanimously agreed that the time needed to fill in information is minimal, and therefore time savings are at best small. Furthermore, one respondent noted that time savings are limited by the limited awareness that consumer have of the right to data portability.

4.3.3 Greater control

The question whether the right to data portability is important for consumer confidence was a very controversial issue among the forum participants. Some believe that data portability is important in fostering confidence, for instance by providing a guard against abuse of data. Others seem to believe that data portability is not a key aspect of confidence. A lack of awareness of the right is often cited as a reason.

Another group of people seem to find a third way. Although they believe that data portability does not necessarily have a direct influence on confidence, it is seen as a tool for fostering brand loyalty and reputation.

Therefore, the picture is unclear as to whether data portability leads to confidence in the market directly, but it may do so in indirect ways.

"I doubt people will actually be aware of this, and if they are, will probably not fully understand the implications" **LE online forum (2017) International Payroll Manager, retail**

A further consideration is that portability is likely to be used more by more savvy consumers. The consultations conducted for this study suggested that age would be most important determinant (younger individuals being more likely to request porting their data), followed by socio-economic factors. This means that benefits will accrue to some consumer segments more than others.

4.3.4 Increased competition & lower transaction cost

"Data portability dramatically reduces the barrier to switching." **LE consultation (2017) head of analytics, retailer**

The most important effect of data portability is thought to be that it facilitates switching between suppliers of goods and services whose purchase involves the disclosure of personal information. While there is no data on the additional consumer benefits which arise from the right to data portability, one can expect that data portability decreases switching costs and therefore should increase switching itself.

However, since there are no common standards for many types of customer data, the usefulness to data controllers of having access to data from other providers might be quite limited and not comparable to the usefulness of data collected by a firm on its own customers (for example, product codes used in inventory systems are often unique to the retailer). However, it seems likely that this problem can be overcome, either through advanced analytics (potentially provided by third parties) or industry standardisation initiatives[40]. However, the lack of standardisation of (machine-readable) data may delay the impact or lead to differentiated impacts across sectors, depending on the degree of data harmonisation.

Making switching easier has a potentially important distributional effect. One interviewee anticipated that reducing the cost of switching would benefit less savvy consumers disproportionately (consumers who are uncertain about pay-offs) because motivated consumers are more likely to invest time and effort to get better deals; once the required effort drops due to portability, the benefits become available to less engaged consumers.

Despite this, there is existing evidence from different markets on the consumer benefits to switching, which can be used to gauge the effect of portabiltiy more generally[41]. As consumer switching is sector-specific, only sector-specific quantitative estimates are available. We provide illustrative calculations of the potential benefit generated by increased consumer switching in Annex 4. In summary:

- In the **electricity market,** additional benefits arising from easier switching due to data portability[42] (total consumer benefit x percentage increase of benefits from data portability) are estimated to be around £50 million per year in the central scenario.
- For the **market for current accounts,** the Competition and Market Authority (2015) found that by switching to the cheapest current account, the average consumer would save £70 a year. The Current Account Switching Service (CASS), which we interpret as having an effect comparable to that of data portability, results in an estimated benefit of £11 million per year.

[40] According to the WP29 Guidelines: "Personal data are expected to be provided in formats that have a high level of abstraction from any internal or proprietary format. As such, data portability implies an additional layer of data processing by data controllers, in order to extract data from the platform and filter out personal data outside the scope of portability, such as inferred data or data related to security of systems."

[41] Note that sector-specific rules on portability will continue to exist alongside data portability as defined in the GDPR.

[42] Switching to the best tariff

4.3.5 Better/more tailored service from new provider (who is able to use/analyse existing data)

On the side of firms, an important question is whether data portability leads to more access and acquisition of data on consumers from other organisations. Although almost all forum participants agree that the information they have on consumers exists somewhere else – and hence could be imported – most respondent do not envisage that the right to data portability allows their organisation to acquire more data on their consumers, and only half envisage using more data collected by other organisations.

The most important reason cited for not acquiring more data is that the respondent believe they already hold all the information they need.

Similar arguments are made about not using more data collected by other organisations. Reasons cited why firms may want to use more data collected by other firms are the fact that doing so will speed up the customer experience, or because the organisation is too small itself to effectively collect data.

The participants nearly unanimously agree that personal data is the most valuable for portability. This is likely because it is the most used data. One respondent noted that holding data on consumers is going to be less important but that access to data in order to cultivate a relationship with consumers becomes more important. Therefore, it seems that all data on consumers is going to be important, as long as it cultivates the consumer-organisation relationship.

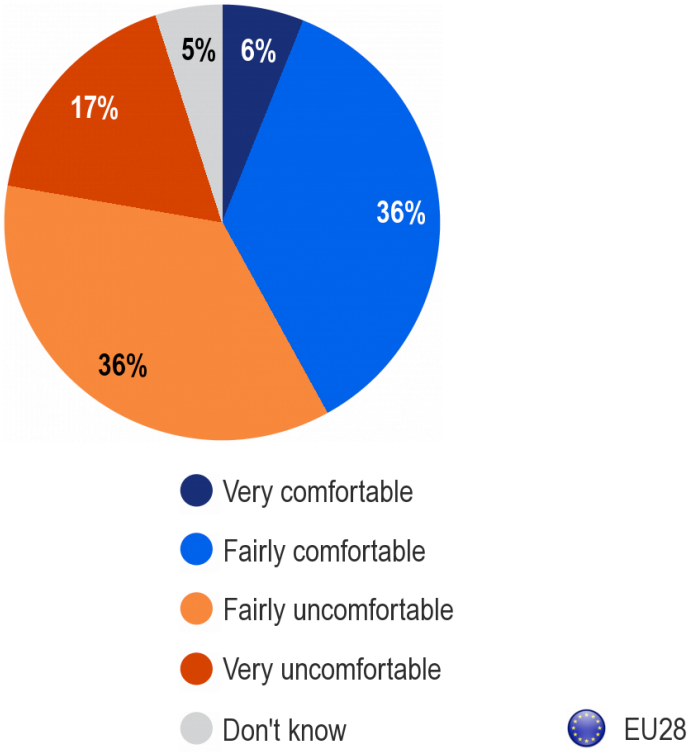
Beyond access to more data, data portability may also change and improve the services provided by organisations. Some respondents believe they already have sufficient data on their consumers and access to more and more detailed information through portability will not improve their services. Others, however, believe that more and more detailed information may allow for services to be tailored better to the client's wishes.

Some uncertainty exists in the economics literature about how much consumers value services that are tailored based on data analytics. Some survey evidence suggests that consumers may be uncomfortable with targeting in relation to online advertising. However, businesses generally see tailoring of services as an unambiguous benefit for consumers.

"Companies that wish to monetize your data or create value (like using your social graph to personalize an experience), will benefit not from owning your data — as so-called "walled gardens" of the past have tried to — but rather by cultivating a relationship with you — one in which they have persistent access to you. The consequences of this way of thinking are profound. Instead of the hostility that comes when users are locked in, it encourages innovation and superior service to ensure that the flow of data doesn't close off." **LE Online forum (2017) Director, retail**

Figure 36 Attitude towards using personal data to tailor advertisement etc.

QB16. As you may know, some online companies are able to provide free services, such as search engines, free e-mail accounts, etc., thanks to the income they receive from advertisers trying to reach users on their websites. How comfortable are you with the fact that those websites use information about your online activity to tailor advertisements or content to your hobbies and interests?



Source: Special Eurobarometer 431 (2015)

Data portability may have a positive impact on improving data consistency. Half of the survey respondents think so, although they are also aware of the fact that data portability may allow "bad data" to propagate[43]. The other half of the respondents do not believe that data portability will improve data consistency.

One consideration raised during the consultations is that, while the GDPR requires data to be made available in a machine-readable, commonly used format, the extent to which the data will actually be useable by other providers after being transferred is in fact highly uncertain: product codes (and other relevant nomenclatures) are in many cases not the same across companies, which can severely limit how a ported dataset can be used. Other aspects of a dataset might be proprietary (e.g. customer segmentation), and it is unclear if this type of data will become portable[44]. The implications of the answer to these questions are momentous.

[43] One issue is that the unit of observation in many commercially relevant settings is the household (loyalty cards, utility bills), rather than the individual who has the right to port their data.

[44] Art 20(4) can be read as including trade secrets or intellectual property, and can be considered before answering a request, but the result "should not be a refusal to provide all information to the data subject". (WP29 Guidelines, p. 12)

4.3.6 Secondary market for data (3rd party services, analysis, switching services)

In business-to-business contexts, it has long been common that customers shop around for a variety of services based on data on their own usage. It is easy to imagine that 3rd party services will emerge that do the same for aggregated consumer data.

Purchasing data, for example is being analysed at the transaction level by companies such as Cardlytics (http://www.cardlytics.com/technology/), and there have been various service attempting to collect and aggregate consumer data and sell it for profit (https://www.nogginasia.com/, People.io (akin to the incentivised panels used by survey companies). It is easy to see a service like this using consumer data captured at source by different providers.

4.4 Auxiliary provisions of the GDPR

Box 7 Summary: Data Protection Officers and maximum fines

Data Protection Officers are seen as increasing awareness of and compliance with legislation. However, DPOs, are not seen as leading to cost reductions for consumers wishing to exercise their rights.

Consumers see the existence of DPOs enabling greater data security in organisations.

Professionals think that fines will have little extra impact on data security, but they may reinforce a security mind set in an organisation.

The loss of consumer trust following a data breach is seen as a much larger problem for organisation than fines.

Consumer trust is directly dependent on the data controller's performance with respect to security and not mediated through the level of fines.

Two further provisions of the GDPR were identified as enabling or supporting the exercise of consumer rights, even though they do not constitute rights in themselves.

4.4.1 Data Protection Officers (DPOs)

The role of Data Protection Officers (DPOs) is to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws; to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.). (ICO)

It is widely accepted that having a DPO does increase the status and priority of data protection within organisations, certainly internally, as having a DPO encourages a culture of awareness and consideration when handling data or setting up systems for recording it. The DPO therefore has a positive impact on data security, quality and accuracy.

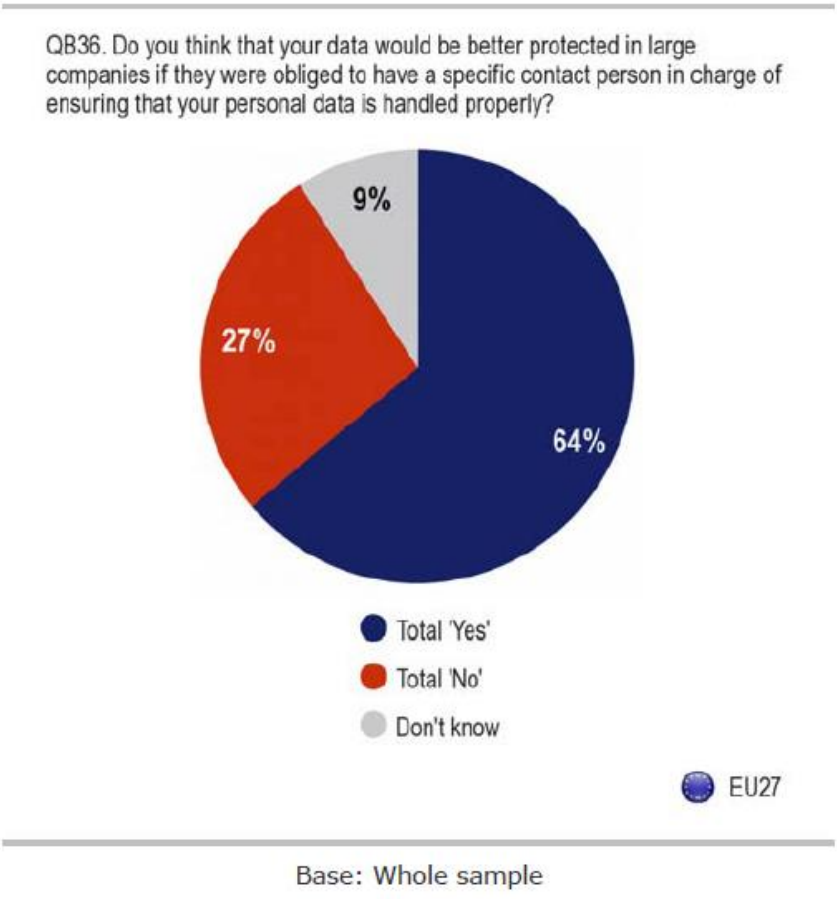
However, having a DPO is not seen to lead to lower costs for individuals wishing to exercise their data-related rights.

"I think it's a positive thing to have a named person with specific responsibility to ensure there is clear accountability and ownership for data protection issues and someone who can help to guide others and ensure the company remains compliant with the GDPR"

— LE Online forum (2017) Marketing manager, business to business

Individuals agree that having a specific individual in charge of data protection would improve data protection within organisations.

Figure 37 Attitude towards Data Protection Officers



Source: Special Eurobarometer 359 (2010)

4.4.2 Maximum fines

Under the GDPR, supervisory authorities are empowered to impose significant administrative fines on data controllers and data processors. Maximum administrative fines of up to €20,000,000 or (in the case of undertakings) 4% of global turnover can be imposed for infringements of the basic

principles for processing, including conditions for infringements of consent (Articles 5, 6, 7 and 9); data subjects' rights (Articles 12-22); the rules on international transfers (Articles 44-49) and others.

The GDPR increases the maximum administrative fines which can be imposed on data controllers and processors. This may lead firms to take data security more seriously. Most participants in the online forums disagree with this. However, this disagreement does not stem from the fact that fines are seen as unimportant, but because firms already take data security seriously in the current situation. Some participants note that data security is already taken very seriously, but that the increase of the maximum fine may reinforce its importance among individual staff members.

"However another essential consideration is how effectively the supervisory function is exercised. If the fines are high and supervision lax then the regulations will not be taken as seriously." **LE online forum (2017) COO and compliance assistance, finance**

Interviewees also made the point that, following an incident such as a serious data breach, the loss of consumer trust would be a much larger problem for them than the fine. This is consistent with a view that consumers care about security of their data, and that their **trust is directly dependent on the data controller's performance with respect to security and not mediated through the level of fines.**

Some participants note that the maximum fine itself is not sufficient to make firms care more about data security. The enforcement of regulation and actual imposition of fines is as important – if not more – than the maximum allowable fine.

"The present maximum fine that the ICO can impose is £500,000 and has been so since 2010. However, the latest statistics from the ICO for quarter 3 show that it issued just one fine for a data breach during the quarter. That was in a case where an employee of an historical society had an unencrypted laptop containing details of donations to the society stolen while working away from the office. The fine? Just £500." **LE online forum (2017) Data protection professional, retail**

Given that most participants believe that their firm already takes data security seriously, it is not surprising that most have not implemented additional security measures in response to the increase in maximum fines.

A second issue concerning fines is whether it actual will lead to behavioural change in consumers. Are they more willing to provide data with larger fines for data breaches? Most participants do not believe this. Participants mainly cite lack of awareness of fines as the reason why consumer may not care about them. However, some participants note that *if* there is public awareness, then fines should strengthen the confidence that people have in the firms storing their data.

Given that most participants believe that higher maximum fines will not lead to behavioural change in consumers, it should not come as a surprise that most feel that higher maximum fines will not benefit them much. Benefits to firms mainly seem to be internal. Staff may take more note of data security practises and be more vigilant.

"This just underlines the importance of data security, it re-enforces to our staff the importance of correct procedure." **LE online forum (2017) Data protection professional, finance**

4.5 Professionals' views on the overall value of GDPR rights

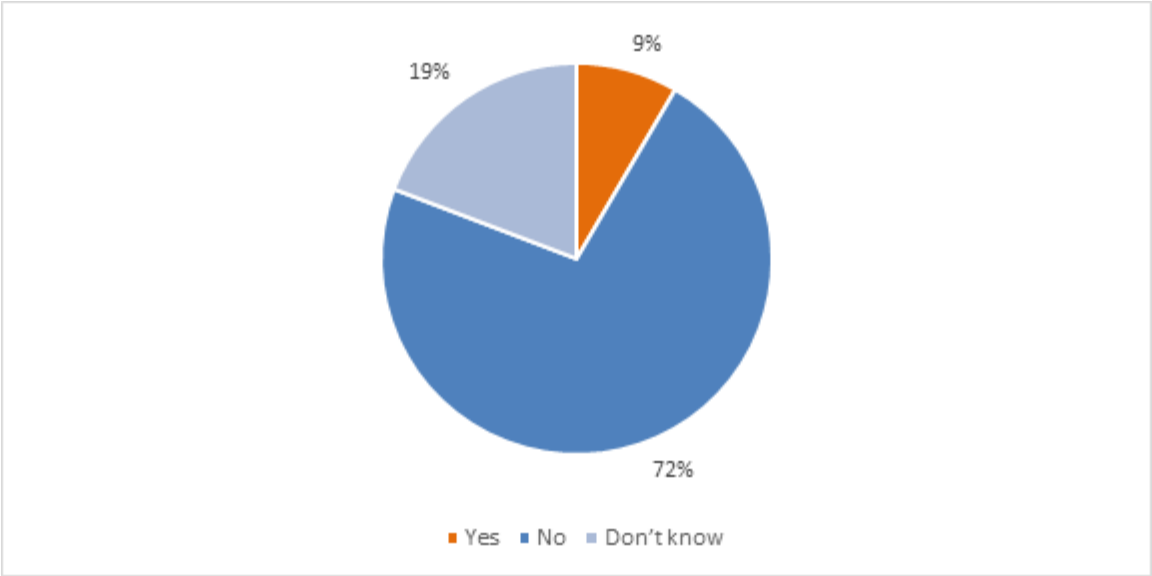
Box 8 Summary: Professionals' views on the overall value of GDPR rights

The rights to access, erasure and data portability are likely to have little impact on firms' profitability. Reasons for this may be that personal data rights are not the most important factor of consumers' decision to provide personal data and that consumers are unlikely to exercise their rights.

Data protection professionals have a hard time pinpointing the likelihood that certain benefits of specific data protection rights embedded in the GDPR will occur, and what the impact will be on their organisation. Survey respondents are overall optimistic that benefits will occur, but less certain that rights will positively impact profitability. For each of the rights, there are some benefits that stand out as more likely to occur. It has not been possible to discount many of the hypothesised benefits as highly unlikely. The potential of the GDPR to give greater control to consumers over their data stands out positively, and is seen as most likely for both the rights to access and erasure.

Given the difficulty of assessing the benefits of specific rights, it is worthwhile to look at the rights embedded in the GDPR as a package. The respondents were asked whether the data rights as a package would increase the profits of their respective firms. As Figure 38 shows, only 21 (9%) respondents thought that the package of rights will increase profits. This is in line with the observation in the previous sections that respondents are less positive about impacts than likelihoods when it comes to specific benefits from personal data rights. **The average increase of profits that these 21 respondents envisage is around 10%, ranging between 1.7% and 40%.**

Figure 38 Do you think that the availability of the right to data portability, access and erasure will increase the profits of your organisation?



Source: LE survey of data protection professionals (2017)

A possible reason why most respondents do not envision an increase of profits is because data rights are not seen as particularly important in consumers' purchasing decisions. Respondents were asked to rate the importance of different factors in the consumer's decision to undertake purchases that involve the disclosure of personal data on a 0-10 scale (0 being not important at all to 10 being very important). The results are presented in Figure 39.

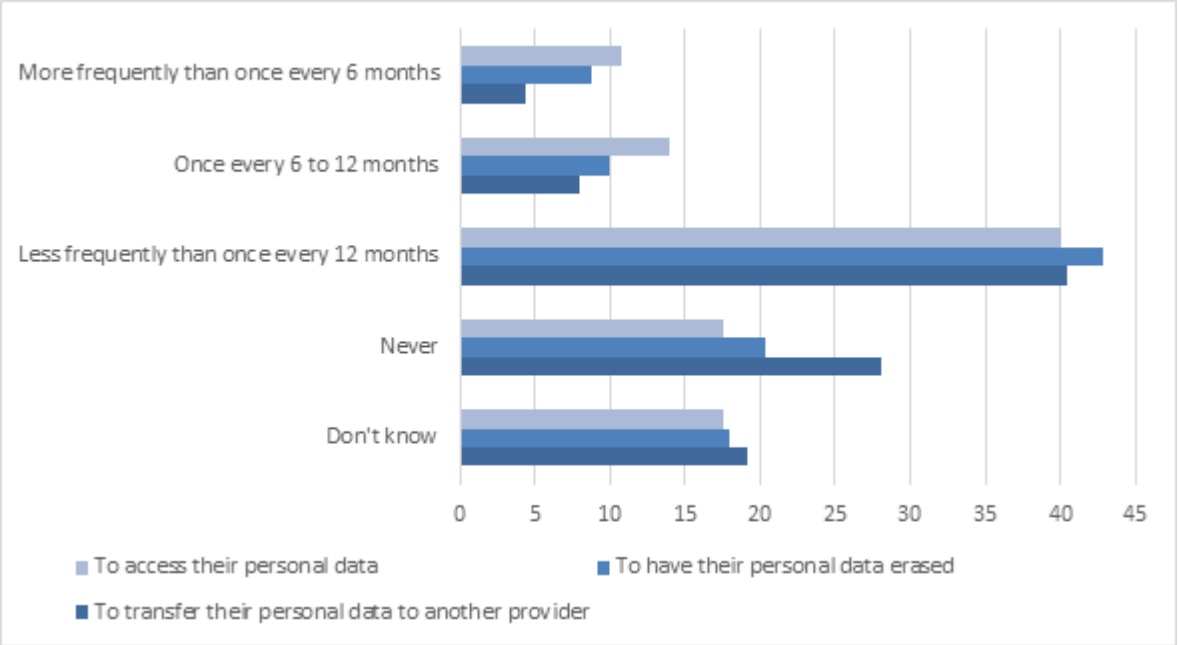
Figure 39 Average importance of different factors in the consumer's purchasing decision

Source: LE survey of data protection professionals (2017)

The package of data rights – and the awareness of the maximum fines – take second place to more universal factors. Reputation and experience are the most important followed by the type of data involved. In terms of the rights themselves, the right of access is seen as most important and the right to data portability as least important.

In addition, respondent do not believe that consumers will exercise their rights frequently. As Figure 40 shows, most respondents do not believe that consumers will use their rights more than once a year, if ever. This is in line with responses from the forums which equally showed that people do not expect consumers to exercise their data protection rights. However, consumers may value data rights because of the knowledge that they can exercise them if they need to, rather than because they expect to use them regularly.

Figure 40 How frequent do you think consumer will ask:



Source: LE survey of data protection professionals (2017)

4.6 Comparison of consumers' and professionals' views

Box 9 Summary: Comparison of consumers' and professionals' views

Both the consumers and data protection professionals rank the personal data rights as least important for the decision to give out personal data, but consumers make less distinction between data rights and other factors.

Professionals expect the rights to be exercised more frequently than consumers.

There is no clear relation between the awareness that consumers have of data rights and the impact that these rights have on profitability of firms.

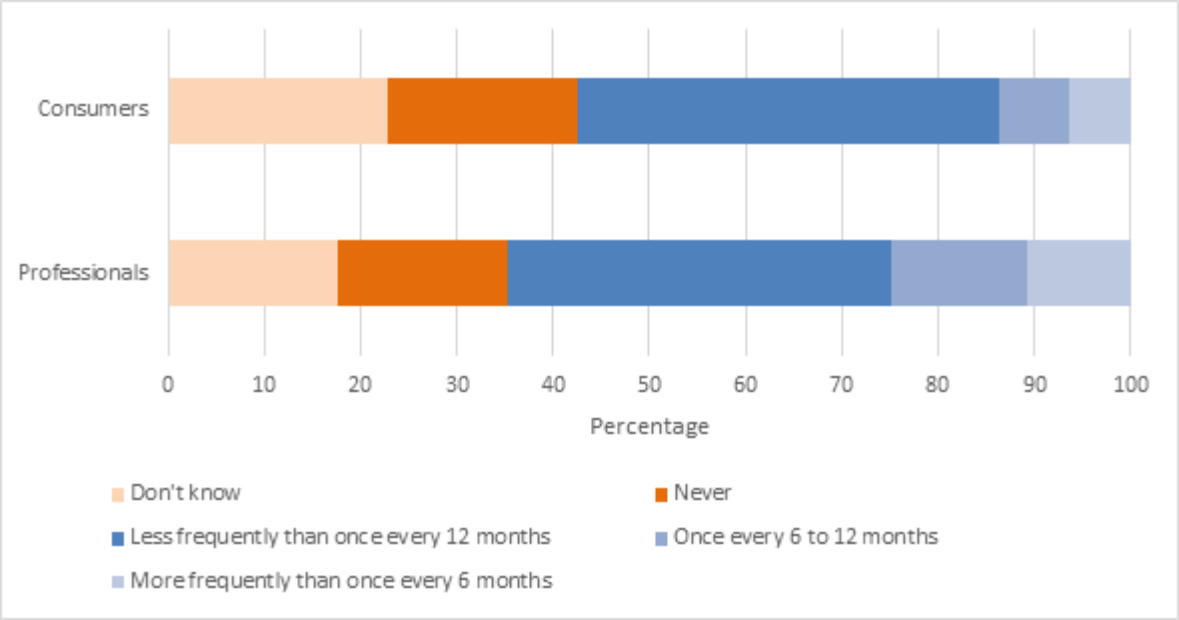
The surveys undertaken for this study were designed to allow comparison of different stakeholder groups. The first such comparison can be made with regards to the importance that data rights have in the consumer's decision. Figure 41 presents the results in the same graph. The figure shows that consumers are more optimistic about the importance of the different elements in the decision to disclose personal data and are make less of a distinction between "traditional" factors such as reputation and the data rights. Given that the consumers are the one's ultimately making the decision, this suggests that the consumer benefits of the GDPR rights might be higher than anticipated by the data professionals.

Figure 41 Importance of data rights in the consumer decision

Source: LE surveys of data protection professionals and consumers (2017)

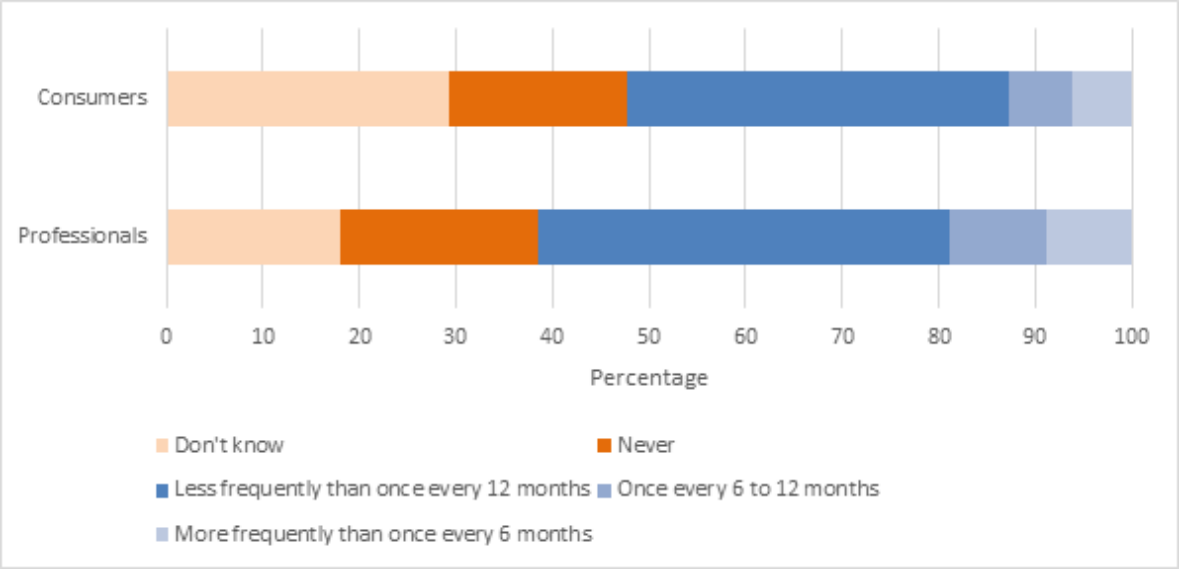
The second comparison is looks at the frequency with which professionals and consumers expect the rights to be exercised. The results are shown in Figure 42, Figure 43 and Figure 44.

Figure 42 Frequency of using: right of access



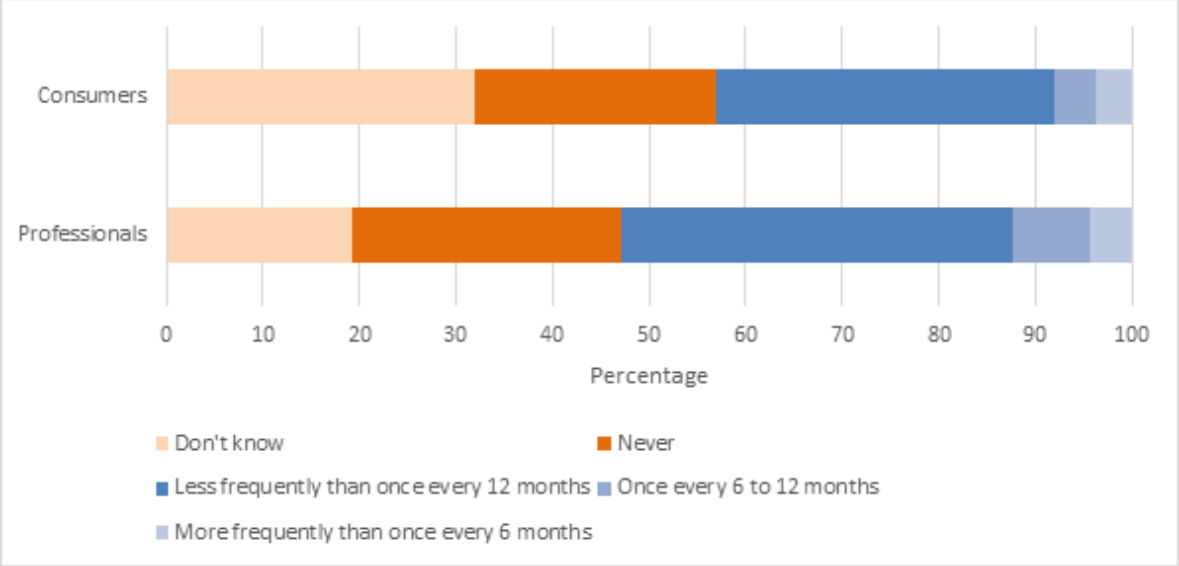
Source: LE surveys of data protection professionals and consumers (2017)

Figure 43 Frequency of using: right to erasure



Source: LE surveys of data protection professionals and consumers (2017)

Figure 44 Frequency of using: right to data portability

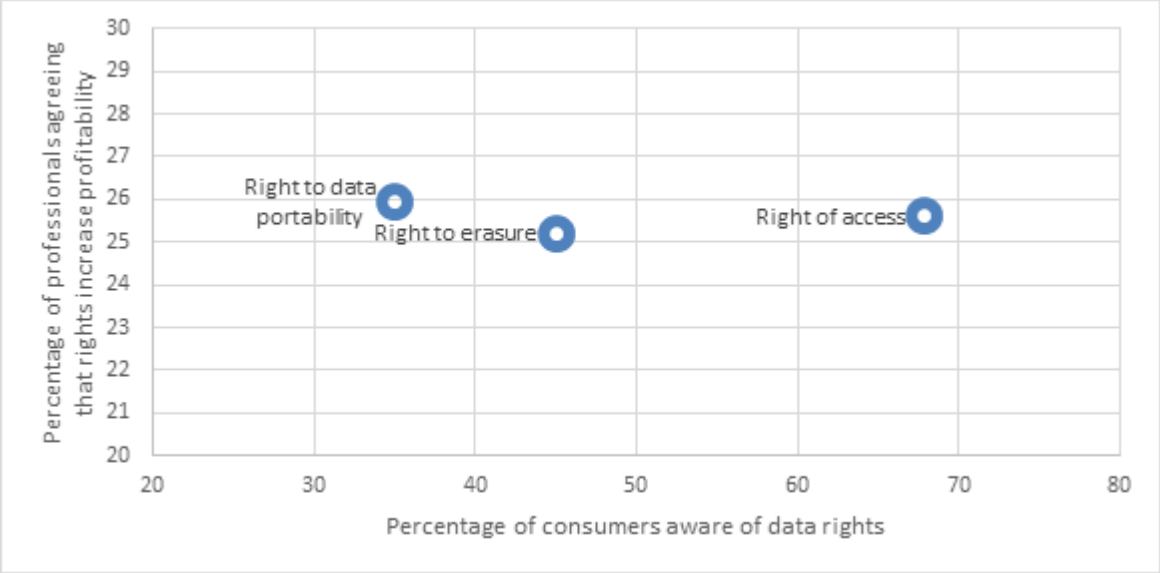


Source: LE surveys of data protection professionals and consumers (2017)

In the previous sections, we already saw that both the data professionals and consumer expect their rights to be exercised infrequently. From the figures above, it seems that data professionals expect the rights to be used with higher frequency than consumers. They also seem to be better able to make this judgement, as evidenced by the lower proportion of "don't know". This finding stands in contrast with the finding on the importance of rights in the consumer decision. Professionals are probably better suited to make this assessment as they should be more aware of how often rights have been exercised in the past. The evidence supports the view that consumers value data protection rights even if they don't exercise them.

Combining the two surveys also allows us to assess whether consumer awareness of a given GDPR right has an impact on additional profitability resulting from that same right. Figure 45 plots, for each of the GDPR rights, the percentage of consumers who are aware of the rights versus the percentage of data professionals who either agree or strongly agree that benefits that come with these rights positively impact profitability, averaged over the benefits for which these opinions have been elicited (see Figure 21, Figure 25 and Figure 34). There is no clear relation between awareness and increased profitability of rights. Again, this points to a tacit understanding that the existence of the rights, rather than informed consumers, drive benefits.

Figure 45 Impact of awareness on profitability



Source: LE surveys of data protection professionals and consumers (2017)

5 Conclusions: GDPR rights as a safety net for digital markets

Box 10 Summary: Conclusions: GDPR rights as a safety net for digital markets

GDPR sets incentives & creates mechanisms that reduce the risk of lapses in data security & misuse of personal data ex ante and mitigate their effects ex post.

A strong data protection framework contributes to the context in which consumers place their trust in transactions that involve disclosure of personal data.

Consumers place a high value on legal protections.

Awareness and exercise of rights is limited: the impact of GDPR does not depend on consumers actively managing their personal data.

Few businesses expect direct (commercial) benefits as a result of GDPR.

Direct benefits from consumer switching are plausible and potentially large.

The effect of increased transparency combined with data portability is not well understood and highly uncertain, but likely to be transformative in certain applications.

Overall, the evidence is compatible with the view that data protection rights, while not a key driver of consumer confidence, function as a contextual factor that complements other, more direct drivers (notably experience and reputation of the counterparty), and, crucially, serves to prevent a systemic loss of confidence in the case of data breaches.

5.1 Summary of the empirical evidence

The research undertaken for this study revealed a **consistently high valuation of GDPR rights by consumers** and a high level of **agreement from professionals that these rights will have specific benefits** (such as greater consumer control, time savings, the emergence of secondary markets for personal data, etc.) depending on the rights in question.

The consumer choice experiment finds that individuals are willing to forego savings of roughly 5% to 10% on weekly spending on shopping, monthly spending on electricity or monthly spending on health insurance in order to have the rights described in the GDPR. This large valuation indicates that individuals are generally happy with the package of rights they have and that they should be

compensated significantly for these rights to be taken away. Furthermore, the existence of maximum fines for non-compliance with the law is highly valued. This high valuation may be interpreted as an implicit insurance against things going wrong. Individuals are willing to pay for the existence of punitive action, which should deter non-compliance.

Data rights are seen by consumers as almost as important as brand reputation, past experience and the type of data required in the decision to give out personal data, with data rights only seen as marginally less important. Consequently, consumers are more optimistic about how important data rights are in these decisions than the professionals.

At the same time benefits to consumers are not necessarily predicted to translate to increased profitability of firms, both for specific benefits and rights and for the package of rights in general. Only 21 of the 250 of the professionals surveyed predict that the package of rights to data portability, erasure and access will increase their profitability.

Overall, data professionals show a high degree of uncertainty when asked to assess the benefits of GDPR data rights. It is noteworthy that the in-depth interviews revealed a surprising lack of imagination and preparedness in terms of the more far-reaching impacts of GDPR, especially second-order effects such as the emergence of new data-centric business models and privacy & and data protection as a competitive advantage.

The benefits of GDPR rights do not depend on consumers exercising their rights frequently. Both consumers and professionals believe that rights will be exercised at best infrequently. In part, this is likely due to the lack of awareness of the existence of data rights – less than 50% of respondent were aware of the rights to erasure or data portability – and to a lesser degree the lack of awareness that rights are needed with people not realising that personal data are collected in certain circumstances.

5.2 A theory of the role of trust in digital markets

Trust is conceptualised as confidence to carry out a transaction that involves the disclosure of personal data.

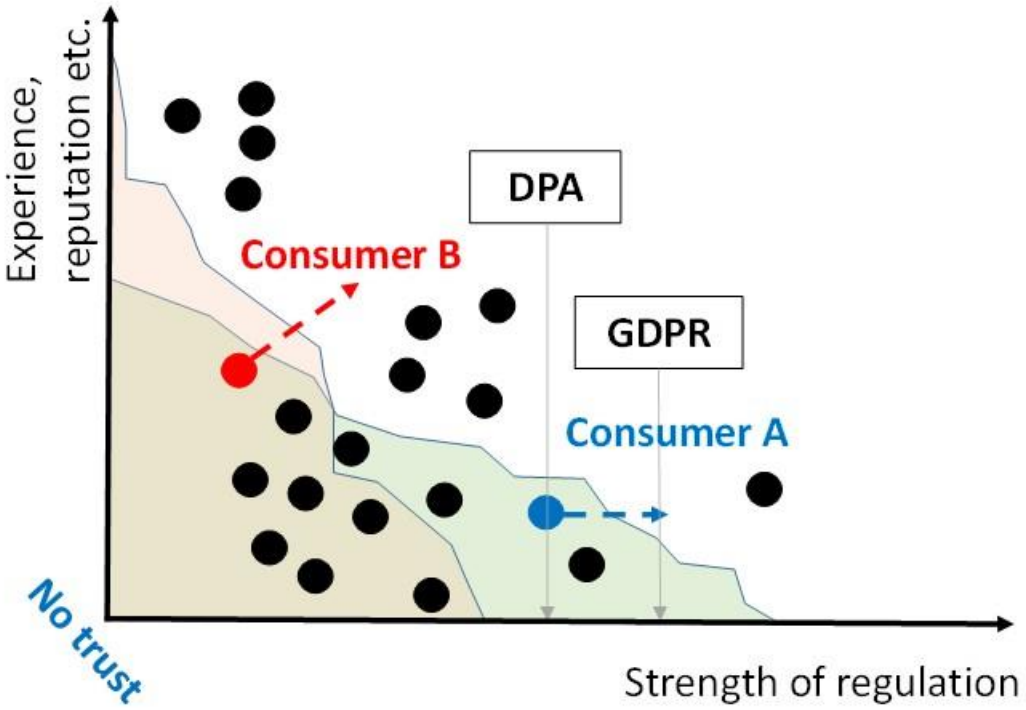
The provision of trust comprises (…) a forced option, a situation in which there is no possibility of not choosing: either A trusts B to achieve C, or A cannot have C.

From a rational choice perspective, social institutions, such as the prevailing regulatory framework, matter because they are parameters in the calculation of whether or not to trust. Luhman (1979, p. 34): “Legal arrangements which lend special assurance to particular expectations and make them sanctionable (…) lessen the risk of conferring trust.” “The apparent basis on which trust is given is necessarily various, including, for instance, the other’s reputation, appearance, past performance, expert qualification or certification, as well as situational rule governance, availability of negative sanctions and so on”. “Claims to trustworthiness are part of the context in which trust is given, not its basis” (Barbalet, 2006, p. 9).

Experimental studies have shown that transacting based on confidence/trust (the counterparty's "tendency to keep promises") can increase social surplus if the alternative, relying on complete contracts, is costly (Chen, 2000)[45].

We can revisit the multi-dimensional model of trust[46] from Section 2.2 to characterise the impact of the GDPR on trust-enabled actions by consumers as follows:

Figure 46 Hypothesis 1: GDPR drives consumer confidence



Note: Transactions can only take place outside the "confidence boundary" (the coloured area in the figure above). The location of the boundary can vary across consumers and across counterparties/transaction types

Source: LE

As before, the confidence boundary demarcates the level of confidence necessary for transactions to take place[47]. Confidence can come from the strength of the regulation ("the context in which trust is given", see above) as well as from the consumer's own experience, the reputation/brand of the counterparty[48], etc. For consumers inside the boundary, a strengthening of the regulation can increase confidence sufficiently to get to a point beyond, where transactions are possible (Consumer A). However, the surveys carried out for this study show that reputation, experience and the

[45] Also, as Beresford et al. (2010) point out, the enforcement of contracts runs into problems because "many contracts involving personal data are incomplete or highly opaque, as they typically lack clear-cut information about secondary uses and sharing of personal information".

[46] Based on Khodyakov (2007).

[47] One interesting modification suggested by one respondent (representing a major retailer) was that GDPR might shift the confidence threshold outwards, by making issues of data protection more salient to consumers.

[48] "(…) more than 75% of consumers are more willing to share personally identifiable information (PII) with brands that they trust than those they don't know (…). https://www.ama.org/publications/eNewsletters/Marketing-News-Weekly/Pages/Data-Sharing-Cheat-Sheet-Columbia-Business-School.aspx

sensitivity of the data that is being disclosed are all stronger factors consumer's purchasing decision on average than specific rights (see Figure 39, p. 56)[49].

Professionals to whom we showed this framework generally agreed with it, however, movements along the 'strength of regulation' axis were seen as speculative, because:

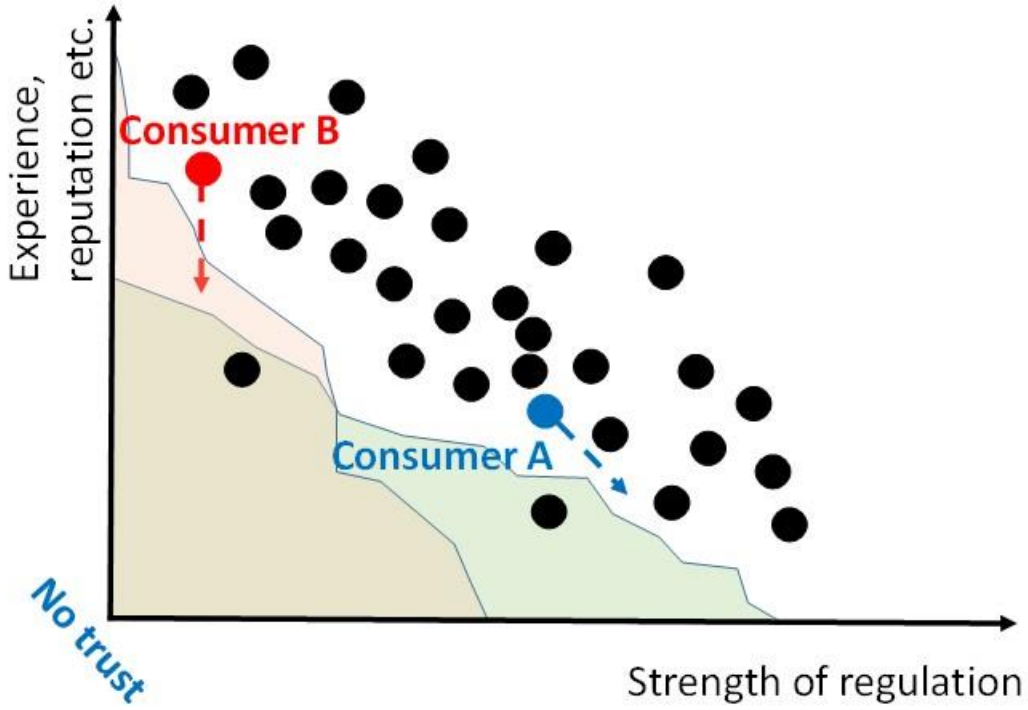
1) consumers are largely unaware of the regulatory framework (see above); and
2) GDPR represents an incremental, rather than a radical change.

In addition, most consumers are already 'above the threshold', i.e. they currently engage in transactions that involve the disclosure of personal data (see Section 2.2.1). Consumer experience (high standards of data security and data protection) was seen by interviewees as the crucial variable companies are trying to control. Scenarios in which consumers might slip below the confidence threshold may be instances of data loss or other adverse publicity around a company's handling of consumer data (i.e. a movement down the vertical axis). It is in this context that the GDPR (the strength of the regulatory framework) has the clearest impact**: a stronger regulatory framework is likely to mitigate the effect of a localised loss of trust** (i.e. a data breach affecting a specific data controller), by reassuring consumers that companies *in general* are incentivised (through rights that allow user control etc.) to keep data safe, and to react to a loss event by strengthening security.

This situation is shown in Figure 47: A loss of consumer trust based on the performance of the data controller such as a data breach results in some consumers falling below the minimum level of confidence needed to transact (Consumer B). A strong regulatory framework mitigates this loss of trust (Consumer A, so that transactions can continue to take place (or confidence recover more quickly).

[49] However, it is possible that the strength of the regulatory framework as a whole has a greater impact than any individual rights.

Figure 47 Hypothesis 2: GDPR helps maintain consumer confidence



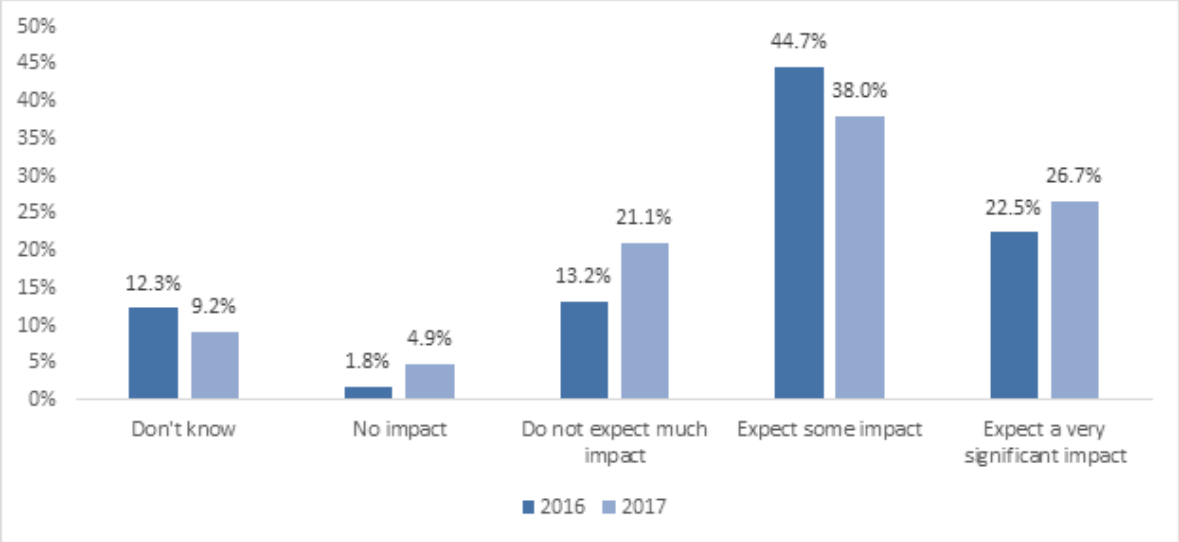
Note: Transactions can only take place outside the "confidence boundary" (the coloured area in the figure above). The location of the boundary can vary across consumers and across counterparties/transaction types

Source: LE

The context here is the well-established fact that data loss is a significant drag on a companies' reputation, with a plurality of business respondents to a 2017 survey (Figure 48) expecting an impact on their reputation following an episode involving data loss[50].

[50] For further evidence see for example Campbell et al. (2003) on negative reaction of share prices to news of security breaches

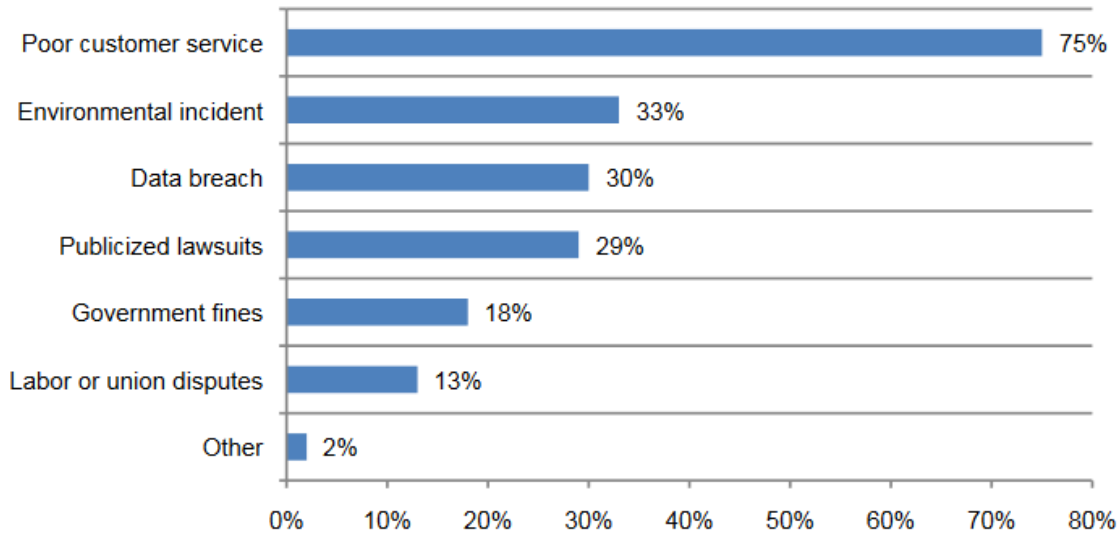
Figure 48 Impact on business and reputation of data breaches or loss



DataIQ (2017), Figure 5.4, p. 19. Based on 220 responses from an online survey of members of the DataIQ community and also to decision-making marketers in a UK online panel in February 2017.

Additional survey evidence (Figure 49) shows that breaches are in the top 3 of incidents that affect reputation.

Figure 49 The incident that would have the greatest impact on a company's reputation



Note: 2 responses permitted

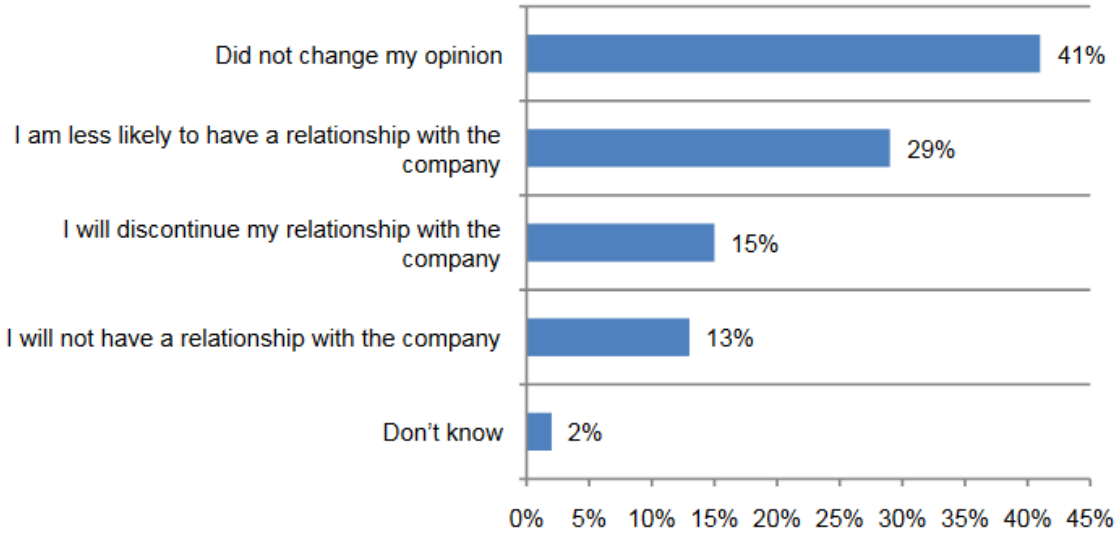
Source: Ponemon Institute (2014)

This implies that **the greatest benefit of the GDPR is not what it enables, but what it prevents, namely a collapse in confidence** after the direct drivers of trust (above all consumers' experience of things not going wrong) have failed. Where the risk of exploitation is reduced (and several GDPR

measures serve this purpose, from consent and use limitation requirements to access rights and breach notification), uncertainty is reduced, which leads to more cooperative behaviours[51].

The hypothesis that **a strong regulatory framework, including sanctions for culpable negligence in the treatment of customer data, acts as a backstop that enables customer confidence to bounce back after an incident** is consistent with the evidence. For example, only a small fraction of (US) respondents in the Ponemon Institute's 2014 study on customer reactions to data loss events discontinue the relationship with a provider after such an episode (Figure 50).[52]

Figure 50 How did reading about the data breach affect your opinion about the company?



Source: Ponemon Institute (2014)

The consensus in the industry appears to be that even notorious data breaches have only a limited impact on the companies involved:

"(…) Target's breach, culminating in the loss of over 100 million customer records, saw the retailer's stock drop 10 percent afterwards. But by February the retailer had experienced its highest percentage stock price regain in five years.

There are other notable examples; Sony Pictures Entertainment saw its stock price keep growing following the announcement of its breach in 2014, while stock prices at JP Morgan Chase were stable following the breach and then rose shortly after. EBay, closing at $51.88 after breach on 21 March, grew to $59.74 exactly a year later.

[51] "The minimum trust threshold will depend on the party's own tolerance for the risk of exploitation by the other side". Stephen Flowerday, Rossouw von Solms:(2006). Trust: An Element of Information Security. In Fischer-Hübner, et al. (Eds) (2006), p. 92.

[52] Note again that there seems to be a large discrepancy between what consumers say they would do and what they do in practice. In a hypothetical scenario, Semafone (2014) report the following percentages of people who stated that they were "not at all likely" or "not very likely" to do business with an organisation which had suffered breaches involving the following types of personal data:

Credit or debit card details	87%
Home address:	83%
Telephone number:	80%
Email address:	76%

Amar Singh, former CISO at News International and founder of Give01Day, told CSO Online that this is because breaches have no long-lasting effects: "Let's be honest, a cyber-attack is not having life impact." (Drinkwater, 07 January 2016)

And there is some survey evidence that knowledge of the data protection framework (but not GDPR specifically) enhances perceptions of confidence:

"those consumers who lack any awareness of a law protecting their data are more likely to be negative than positive - 23.4 per cent are worried or think organisations do not do enough compared to 12.1 per cent who believe some of their data is safe or are very confident. By contrast, where consumers claim to be fully aware, 6.4 per cent have a level of confidence compared to 3.3 per cent who do not" (However, the self-reported knowledge of the GDPR in particular does not influence perceptions on the safety of personal data)." (DataIQ (2017), p. 11)

Finally, it appears that the some of the key measures in the GDPR coincide with the actions that consumers would like to see following a data breach. A 2016 survey of 6,000 adults in the US[53] "asked participants to identify actions they would recommend and actions they would discourage on the part of companies after a data breach. The steps that would highly satisfy most respondents were

1) take measures to ensure that a similar breach cannot occur in the future (68%),
2) offer free credit monitoring or similar services to ensure that lost data are not misused (64%), and
3) notify consumers immediately (63%).

All three of these actions were valued more highly than receiving financial compensation for the inconvenience". Note that 1) is incentivised strongly by GDPR (through fines), while 3) is a mandatory requirement. This further supports the view that GDPR has an important role in mitigating the effects of data breaches on consumer confidence ex post (in addition to creating incentives that make breaches less likely in the first place, such as fines).

Overall, the evidence is compatible with the view that data protection rights, while not a key driver of consumer confidence, function as a contextual factor that complements other, more direct drivers (notably experience and reputation of the counterparty), and, crucially, serves to prevent a systemic loss of confidence in the case of data breaches.

[53] Ablon et al. (2016)

References

Ablon L., Heaton, P., Lavery, D. C. and Romanosky, S. (2016). *consumer attitudes toward data breach notifications and loss of personal information* (Rand Corporation Research Report). Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf

Acquisti, A., Taylor, C. and Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature 2016, 54(2),* 442–492. http://dx.doi.org/10.1257/jel.54.2.442.

Article 29 Data Protection Working Party (2016a). *Guidelines on the right to data portability.* WP 242. Retrieved from http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Article 29 Data Protection Working Party (2016b). *Guidelines on Data Protection Officers ('DPOs')*. WP 243. Retrieved from http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Barbalet, J. (2006). *A characterisation of trust and its consequences.* Social Contexts and Responses to Risk Network (SCARR) Working Paper 13-2006. Retrieved from: https://www.kent.ac.uk/scarr/publications/Barbalet%20Wk%20Paper(2)%2013.pdf

Campbell, K., Gordon, L. A., Loeb, M. P. 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), 431–48.

Campbell, J., Goldfarb, A. and Tucker, C. (2015). Privacy regulation and market structure. *Journal of Economics and Management Strategy,* 24(1), 47–73.

Cave, K. (03 February 2017). *GDPR probably won't decimate businesses but it might leave some burned* (blog post). Retrieved from IDG Connect website: http://www.idgconnect.com/blog-abstract/24273/gdpr-probably-won-decimate-businesses-leave-burned

Chen, Y. (2000). Promises, trust, and contracts. *Journal of Law, Economics, & Organization,* 16(1), 209-232. doi:https://doi.org/10.1093/jleo/16.1.209

Christensen et al (2013) *The impact of the Data Protection Regulation in the E.U.*

Ciriani (2015) *The Economic Impact of the European Reform of Data Protection* and

Competition and Market Authority. (2015). Retail banking market investigation: Summary of provisional findings report. Retrieved March 1, 217, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470032/Banking_summary_of_PFs.pdf

Crosby, L.A. and Zak, P.J. (2015). The neuroscience of brand trust. *Marketing Management.* May, 22–23. https://www.ama.org/publications/MarketingNews/Pages/the-neuroscience-of-brand-trust.aspx

Ctrl-Shift (2014). Personal Information Management Services: An analysis of an emerging market Understanding the impacts on UK businesses and the economy (Report). Retrieved from https://www.ctrl-shift.co.uk/insights/2014/06/16/personal-information-management-services-an-analysis-of-an-emerging-market/

DataIQ In association with DQM GRC (2017). *General Data Protection Regulation 2017 - Identifying its impact on marketers and the consumer's moment of truth – No. 1: Protection* (DataIQ Research Report). Retrieved from http://www.dataiq.co.uk/land/2017-gdpr-impact-research-report-protection

Drinkwater, D. (07 January 2016). Does a data breach really affect your firm's reputation? (Feature). Retrieved from CSO website http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html

European Commission (18 June 2015). *Digital Agenda Scoreboard 2015: Most targets reached, time has come to lift digital borders.* Retrieved from: https://ec.europa.eu/digital-single-market/en/news/digital-agenda-scoreboard-2015-most-targets-reached-time-has-come-lift-digital-borders

European Commission (2012). Commission staff working paper (GDPR Impact Assessment, SEC(2012) 72 final). .

European Commission (2016a). *Digital Agenda Scoreboard reports - Use of Internet Services by Citizens in the EU 2016* (presentation). Retrieved from https://ec.europa.eu/digital-single-market/en/download-scoreboard-reports

European Commission (2016b). *EU Data Protection Reform - What benefits for businesses in Europe?* (Fact sheet). Retrieved from http://ec.europa.eu/justice/data-protection/document/factsheets_2016/data-protection-factsheet_01a_en.pdf

European Commission. (2010). *The functioning of retail electricity markets for consumers in the European Union.* Final Report. Retrieved February 28, 2017, from http://ec.europa.eu/consumers/archive/consumer_research/market_studies/docs/retail_electricity_full_study_en.pdf

European Commission. (n.d.). *Second consumer market study on the functioning of the retail electricity markets for consumers in the EU.* Retrieved February 28, 2017

Feri, F., Giannetti, C. and Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior and Organization*, 123, 138–48.

Financial Conduct Authority. (2015). *Making current account switching easier: The effectiveness of the Current Account Switch Service (CASS) and evidence on account number portability.* Retrieved March 1, 2017, from https://www.fca.org.uk/publication/research/making-current-account-switching-easier.pdf

Fischer-Hübner, S., Rannenberg, K, Yngström, L. and Lindskog, S. (Eds) (2006). *Security and privacy in dynamic environments* (Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22-24 May 2006, Karlstad, Sweden). doi:10.1007/0-387-33406-8

Furlong, D. (1996). The conceptualization of 'trust' in economic thought. *IDS Working Paper 35.* Retrieved from: https://www.ids.ac.uk/files/Wp35.pdf

Hann, I.-H., Hui, K. L. Lee, S.-Y. T. and Png, I. P. L. (2008). Consumer privacy and marketing avoidance: a static model. *Management Science,* 54(6), 1094–1103.

Khodyakov, D. (2007). Trust as a process: a three-dimensional approach. *Sociology,* 41(1), 115-132.

London Economics (2013). *Implications of the European Commission's proposal for a general data protection regulation for business* (Report to the Information Commissioner's Office). Retrieved from https://ico.org.uk/media/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf

Luhmann, N. (1979). *Trust and power*. Chichester: Wiley.

McKinsey Global Institute (2016). *Digital Europe: Realizing the continent's potential* (Report). Retrieved from: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-europe-realizing-the-continents-potential

Ministry of Justice (2012). *Proposal for an EU Data Protection Regulation – Impact Assessment (IA).*

Norberg, P. A., Horne, D. R. and Horne, D. A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs,* 41 (1), 100–126.

Office for National Statistics. (2016, February 17). Retrieved March 6, 2017, from Total number of households by region and country of the UK, 1996 to 2016: https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/families/adhocs/005374totalnumberofhouseholdsbyregionandcountryoftheuk1996to2015

Ponemon Institute (2014). The aftermath of a data breach: consumer sentiment (Research Report sponsored by Experian Data Breach Resolution). Retrieved from http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

Rainie, L. and Duggan, M. (2016). *Privacy and information sharing.* Pew Research Center. Retrieved from:

Rao, J. M., and David H. Reiley (2012). The economics of spam. *Journal of Economic Perspectives,* 26(3), 87–110.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

Richard H. McAdams (2008). Beyond the prisoner's dilemma: coordination, game theory, and the law. University of Chicago Public Law & Legal Theory Working Paper, No. 241.

Semafone (2014). *86% of customers would shun brands following a data breach* (news item). Retrieved from https://semafone.com/86-customers-shun-brands-following-data-breach/

Skyrms, B. (2001). The stag hunt (Presidential Address, Pacific Division of the American Philosophical Association*). Retrieved from http://www.socsci.uci.edu/~bskyrms/bio/papers/StagHunt.pdf*

Stone, E. F., and Stone, D. L. (1990). Privacy in organizations: theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management,* 8(3), 349–411.

Tamir, D. I. and Mitchell, J. P. (2012). Disclosing Information about the Self Is Intrinsically Rewarding. *Proceedings of the National Academy of Sciences*, 109(21), 8038–43.

Taylor, C. R. (2004). Consumer privacy and the market for customer information." *RAND Journal of Economics*, 35(4), 631–50.

Ustaran, E. and Choi, S. (16 December 2016). *Triple GDPR guidance issued by article 29 working party* (Hogan Lovells Chronicle of Data Protection blog post). Retrieved from http://www.hldataprotection.com/2016/12/articles/international-eu-privacy/triple-gdpr-guidance-issued-by-article-29-working-party/

Villas-Boas, J. M. (1999). Dynamic competition with customer recognition. *RAND Journal of Economics,* 30(4), 604–31.

Yamagishi, T. Kanazawa, S., Mashima R. and Terai, S. (2005). Separating trust from cooperation in a dynamic relationship – prisoner's dilemma with variable dependence. *Rationality and Society,* Vol. 17(3), 275–308. doi:10.1177/1043463105055463

Index of Tables, Figures and Boxes

Tables

Figures

Boxes

ANNEXES

Annex 1 Data sources

This annex describes the data sources on which the analysis carried out for this study is based.

A1.1 Online survey of professionals

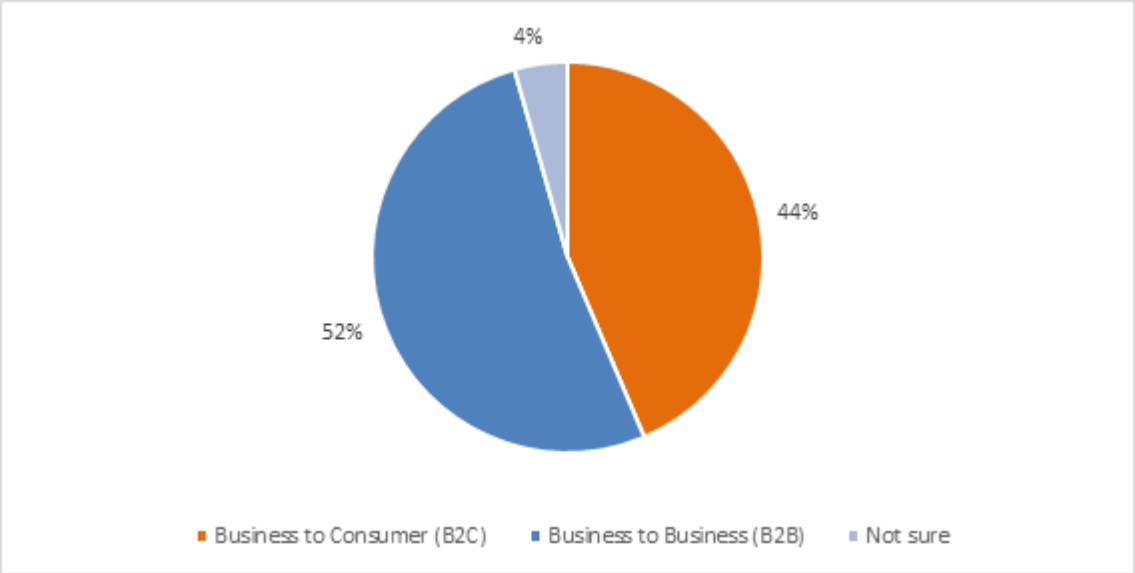
An **online survey** of individuals with data protection responsibilities at their place of work was carried out by YouGov in the last two weeks of March 2017. 250 responses were received.

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 YouGov panel we asked those in full or part time employment to pick out their areas of responsibility. Data protection was one of 29 areas of responsibility listed; others included office supplies, marketing, IT support, customer services, finance, etc. This generated a pool of around 1,350 people with responsibility for data protection. Extra screening criteria excluded the self - employed or single person business and those working in public and not for profit sectors reducing the pool to 840. Invitations to participate were issued at random using the pool of 840 until 250 responses were received.

The sampling strategy means that the resulting sample is **unlikely to be representative** of the UK business population or of the population of data protection professionals in the UK. This means that we cannot be sure how generalisable the survey results are. However, the sample reflects a broad range views in terms of the size, sector and business models (B2B or B2c) of the organisations in which the respondents are employed. The online forums (see below), for which participants were recruited using the same screening approach, further confirm that respondents work with a variety of (personal) data types with varying degrees of sophistication in terms of how the personal data is used in the organisation. The following summary tables indicate the variety of organisation types that are represented in the sample. There is no evidence in the available demographic information that the sample is systematically skewed towards certain organisations types.

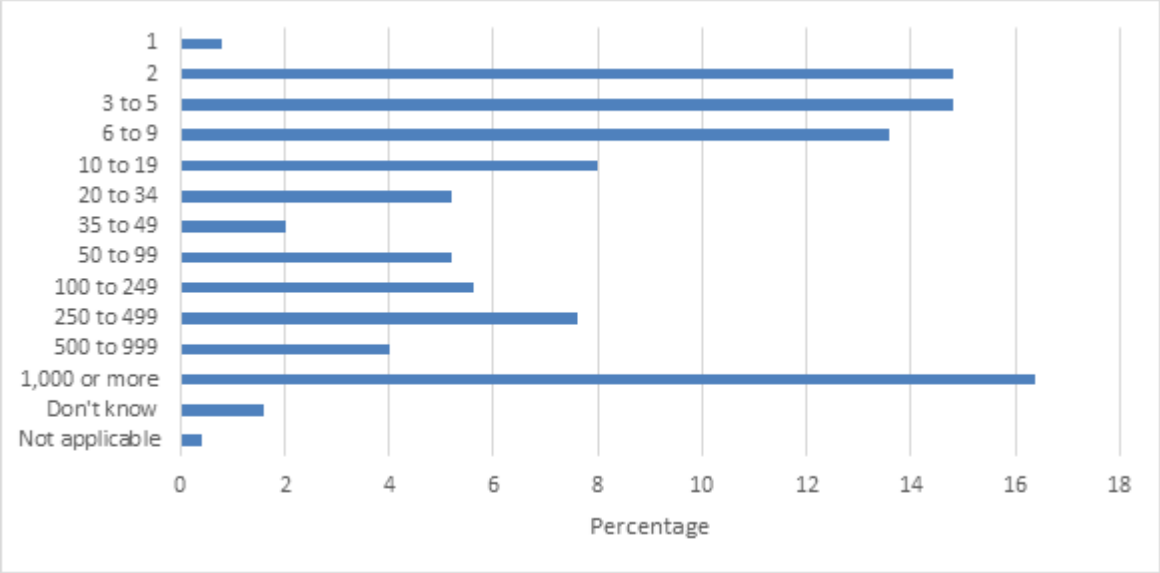
The respondents are split relatively equally between Business to Consumer (B2C) and Business to Business (B2B) professionals (Figure 51), working mainly in small or large firms, with mid-sized firms being less represented (Figure 52). Furthermore, companies represented tend to be at the low end of annual turn-over (Figure 53). The industry sectors represented vary, but with a relatively large representation of financial services, manufacturing, retail and especially IT & telecoms (Figure 54).

Figure 51 Type of business of the respondent



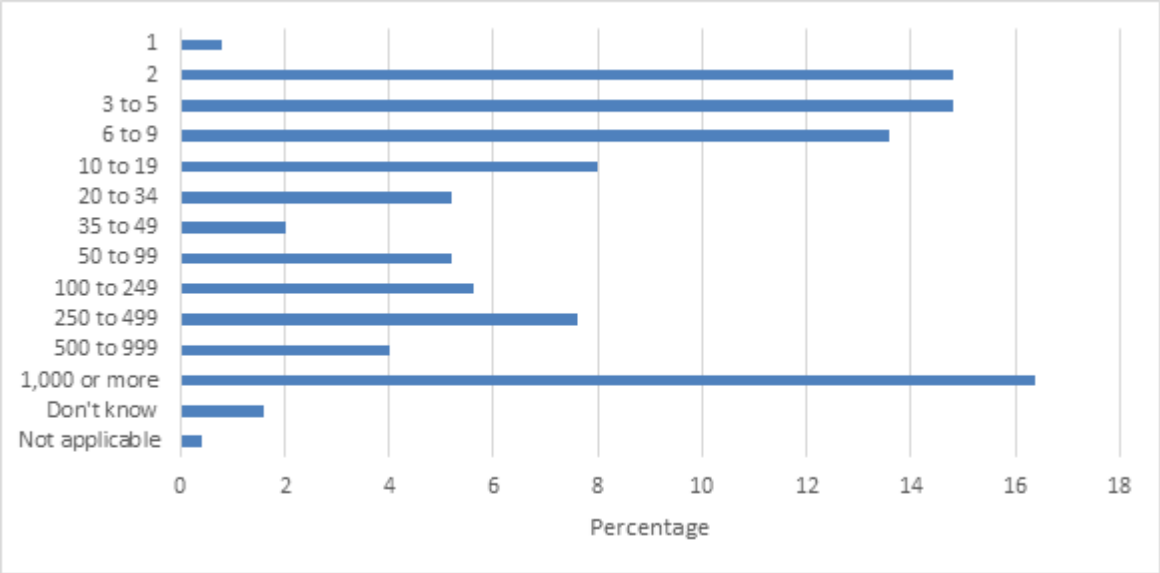
Source: LE survey of data protection professionals (2017)

Figure 52 Firm size



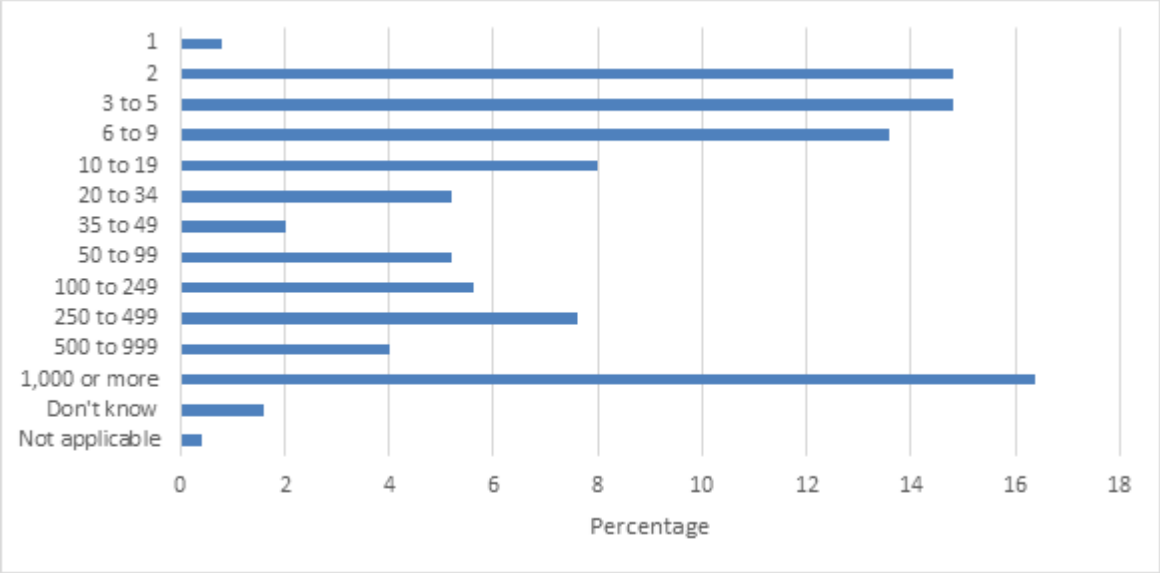
Source: LE survey of data protection professionals (2017)

Figure 53 Annual turn-over



Source: LE survey of data protection professionals (2017)

Figure 54 Industry sector



Source: LE survey of data protection professionals

A1.2 Online survey of consumers (choice experiment)

A **choice experiment** implemented through an online survey was conducted to elicit valuations for the key GDPR rights in three settings: a contract with an electricity provider; a weekly groceries shop and a private health insurance product. In each case, the framing included a trade-off between personal data disclosed to the provider (smart metering data, loyalty card data and health-related data, respectively). 503 responses were received. The sample was drawn **randomly** from YouGov's online consumer panel.

A1.3 Online forums

Three **online forums** were commissioned to run over 4 days, managed by YouGov. The first forum served as a pilot and asked questions about the full set of rights, whereas forums 2 and 3 focused on data portability and access and erasure, respectively (a question on fines was also included). Participants were invited to log in at any time each day (at least once a day for 10-20 minutes) to answer 4-6 daily questions and personal probes.

The three forums contained a mix of participants in terms of business sectors, size and type of organisation (including both private and public sector organisations). Participants were screened to include only individuals with data protection responsibilities at their place of work (using the same approach that was used in the professionals' survey, see above). There were 5-10 participants in each forum, who were recruited via YouGov's online research panel. The forum transcripts are included in Annex 3.

A1.4 Consultation exercise

A focused **consultation exercise** with senior data professionals in UK-based companies was carried out. This was done to ensure that first-hand experience from key industry sectors was fed in to the research. A particular aim was to sense-check the theory-derived value chains. Interviews were conducted with senior data professionals, representing Addison Lee, the Co-operative Group, MoneySupermarket.com, Walgreens Boots Alliance, the British Bankers' Association, a major airline, and other data industry professionals from the current (2017) DataIQ 100[54] list who requested anonymity.

A1.5 Secondary sources

A wide variety of secondary sources was consulted, including:

- Commentary and analysis from law firms on the current understanding of the scope of the GDPR rights under investigation (bearing in mind that there is considerable uncertainty about how DPAs and courts will interpret the rights in practice);
- survey evidence on consumer trust in digital markets, the disclosure of personal data and the role of data protection law in enabling disclosure and market participation;
- evidence from other (non-data) industries on the economic benefit of consumer switching; and
- research literature on the economics of privacy and the determinants of consumer trust.

For details see the references section above.

[54] http://www.dataiq.co.uk/dataiq100

Annex 2 Consumer choice experiment methodology & results

A2.1 Choice environment

The choice experiment set out to test whether the rights to access, erasure and data portability are important in economic decisions where personal data is traded for value. Furthermore, the impact of the existence of a maximum fine for non-compliance with the law has been included as a potential driver for personal data trade. The experiment also sought to attach a willingness to pay valuation to each of the GDPR rights.

In order to do this, a total of 502 respondents completed a choice experiment embedded within an online survey. The choice experiment asked respondents to make a number choices between two alternative options in three different contexts.

The first context required choices between two options for retailer loyalty card schemes, where a discount could be received in return for personal data. Each option varied in terms of the average weekly discount the individual would receive on their food and drink shopping and on the personal data rights associated with the loyalty card scheme. More specifically, the attributes varied were:

- the average weekly discount from the loyalty scheme,
- whether the right of access was granted,
- whether right to data portability was granted,
- whether the right erasure was granted, and
- whether there was a maximum fine for non-compliance[55].

The option to choose neither of the two possible loyalty cards was also available. The screenshot in Figure 55 provides an example of a choice card. Each respondent made 6 choices in this context, where each option for each choice varied in its attributes.

[55] The options for the maximum fine were either "Zero" or "£15 million or 5% of turnover, whichever is greater". These numbers are deliberately different from the maximum fine established in the GDPR.

Figure 55 Choice environment, loyalty card scheme

YouGov

Suppose you have a choice between the two loyalty cards/schemes shown in the table below. Which of these would you choose?

	Loyalty card A	Loyalty card B
Discount you would receive on average per week on your food and drink shopping:	£1.24	£4.81
Under the conditions of service you can:		
Request, free of charge, complete details of the personal data the provider has on you	NO	YES
Copy or transfer your personal data from the current provider to another	YES	NO
Request the deletion or removal of personal data stored by the provider	NO	YES
Fine the provider will face if they process personal data without your consent or do not comply with the above conditions of service:	£15 million or 5% of turnover*	Zero

* Whichever is greater

Choose A Choose B

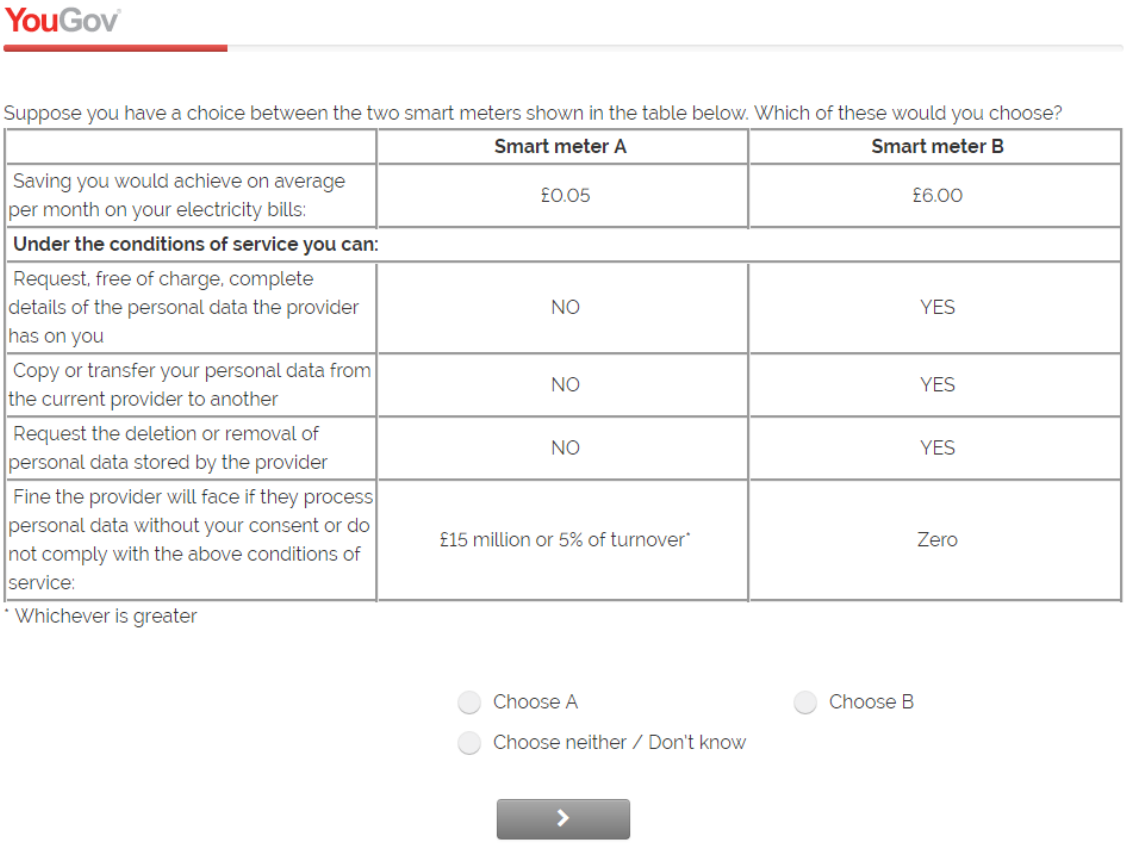
Choose neither / Don't know

Source: LE survey of consumers (2017) Choice experiment

The second context required choices between two options for electricity smart meters, where a smart meter leads to savings on the individual's electricity bill but allows the supplier to obtain personal information. Again the attributes for each option were varied, here according to average monthly savings attained by having the smart meter, whether the various GDPR rights were granted, and whether there was a maximum fine. Figure 56 shows an example of a choice card in this context.

In this context, respondents again made 6 choices, where each option of each choice varied in terms of the attributes and where the option to choose neither was also available.

Figure 56 Choice environment, smart meter

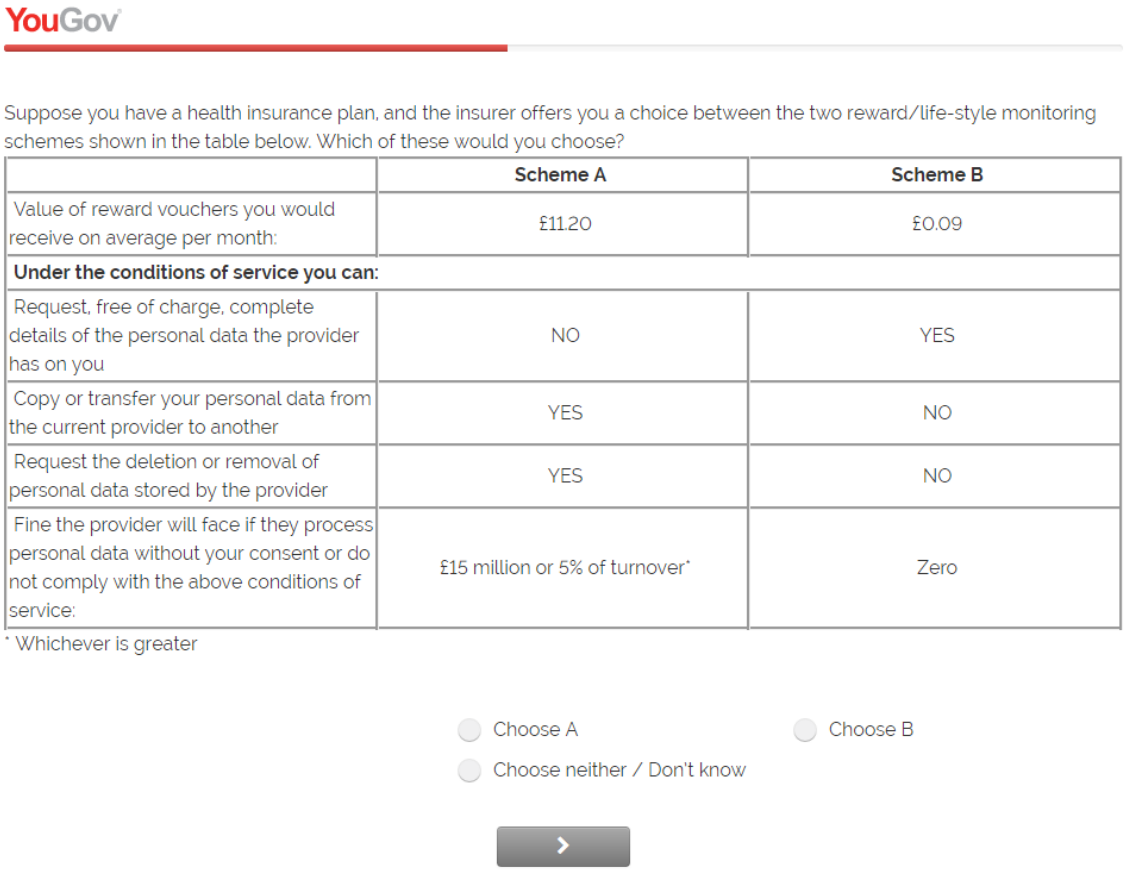


Source: LE survey of consumers (2017) Choice experiment

The third context required choices between two options for reward schemes run by health insurance companies. In these schemes, the insurance company rewards clients who maintain healthy life styles in return for personal information on health (such as how far a client has walked). The attributes for each option were varied in terms of the average monthly value of vouchers received, whether the various GDPR rights were granted, and the existence of a maximum fine. Figure 57 provides an example of a choice card in this context.

In this context, each respondent made 6 choices, where each option for each choice varied in attributes and with the option to choose neither available.

Figure 57 Choice environment, health insurance voucher scheme



YouGov

Suppose you have a health insurance plan, and the insurer offers you a choice between the two reward/life-style monitoring schemes shown in the table below. Which of these would you choose?

	Scheme A	Scheme B
Value of reward vouchers you would receive on average per month:	£11.20	£0.09
Under the conditions of service you can:		
Request, free of charge, complete details of the personal data the provider has on you	NO	YES
Copy or transfer your personal data from the current provider to another	YES	NO
Request the deletion or removal of personal data stored by the provider	YES	NO
Fine the provider will face if they process personal data without your consent or do not comply with the above conditions of service:	£15 million or 5% of turnover*	Zero

* Whichever is greater

Choose A Choose B

Choose neither / Don't know

Source: LE survey of consumers (2017) Choice experiment

A2.2 Analysis

The choices made in the experiment described above lead to information on whether an option was chosen or not. After removing all individuals who at least once chose "choose neither/don't know", this yields data on 11,246 options[56].

The data on these choices are binary (you either do or do not choose an option) and matched (if you choose option A, you automatically do not choose option B). Therefore, the appropriate analysis tool is the conditional logit, with the data on whether an option was chosen as dependent variable and data on the various attributes of the choice as explanatory variables.

The underlying linear regression function used for this is:

$$choice\ option\ x = \alpha_o + \alpha_1 * right\ to\ access + \alpha_2 * right\ to\ data\ portability + \alpha_3 * right\ to\ erasures + \alpha_4 * maximum\ fines + \alpha_5 * discount + \varepsilon$$

[56] Note that each decision by a respondent leads to two different results on choice of options. If a respondent chooses option A, she automatically does not choose option B.

Given that the choice for x is binary, this linear form is subsequently transformed based on the cumulative logistic distribution and estimated as a maximum likelihood estimation. Note that no additional controls have been added to the model.

The coefficients of a conditional logit allow us to tell whether the inclusion of an attribute in any given choice increases (if significantly positive) or decreases (if significantly negative) the probability that an option is chosen. By taking the natural exponent of the coefficient, the odds ratios can be obtained[57]. Odds are the ratio between the probability that an option is chosen and the probability that an option is not chosen, i.e. $odds = \frac{probability}{1-probability}$. The odds ratio for the personal data rights is the ratio between odds under the scenario that any given right does exists and the odds that a right does not exist, i.e. for any option x and personal data right y:

$$odds\ ratio(y) = \frac{p(choosing\ x|y\ exists)/\left(1-p(choosing\ x|y\ exists)\right)}{p(choosing\ x|y\ does\ not\ exist)/\left(1-p(choosing\ x|y\ does\ not\ exist)\right)}.$$

The odds ratio for the discount is defined as the odds of choosing a particular option under a given discount divided by the odds under a discount of £1 less, i.e. (for any option x):

$$odds\ ratio(discount) = \frac{p(choosing\ x|discount + £1)/(1-p(choosing\ x|discount + £1))}{p(choosing\ x|discount)/\left(1-p(choosing\ x|discount)\right)}.$$

Generally, an odds ratio of larger than 1 implies a positive impact of a personal data right or discount on the odds of choosing a particular option, while an odds ratio of smaller than 1 suggests that the data right or discount has a negative impact on the odds of an option being chosen.

Lastly, the coefficients for each of the attributes can be converted into the willingness to pay by dividing the coefficient of the attribute by the coefficient for the discount or savings obtained in the choice. For example, if a_1 is the coefficient for whether the right of access has been granted in a loyalty scheme and a_5 is the coefficient for the average weekly savings in that loyalty scheme, then the willingness to pay for the right of access, in this context, is calculated as a_1/a_5.

A2.3 Regression results

A2.3.1 Loyalty cards

Table 4 provides results on the probability of choosing a loyalty card scheme under different packages of rights, fines and discounts.

Table 4 Impact of rights, fines and discounts on the probability of choosing a loyalty card scheme

	Coef.	P-value	Odds ratio
Right to request complete details of the personal data the provider has on you	0.499	<0.001	1.647
Right to copy or transfer your personal data from the current provider to another	0.137	0.076	1.147
Right to request the deletion or removal of personal data stored by the provider	0.838	<0.001	2.312

[57] I.e. $OR = e^{coefficient}$.

Provider faces a fine of £15m or 5% of turnover for non-compliance	0.937	<0.001	2.552
Discount you would receive on average per week on your food and drink shopping	0.129	<0.001	1.138

Note: The coefficients of the conditional logit model by themselves are not easily interpretable. They tell us whether the inclusion of an attribute in any given choice increases (if significantly positive) or decreases (if significantly negative) the probability that an option is chosen. By taking the natural exponent of the coefficient, the odds ratios can be obtained. See Box 11 for further details on interpreting odds ratios.

Source: LE survey of consumers (2017) Choice experiment

All coefficients are positive and – with the exception of data portability – highly statistically significant. This shows that individuals are more likely to choose a loyalty card scheme if they have the right of access or right to erasure, if there are maximum fines for misuse of data[58], or if they receive larger discounts on their weekly food and drink shopping. The likelihoods can be made more tangible by translating the coefficients to odds ratios (see Box 11). These odds ratios show that fines and the right to erasure are the most important attribute of choosing a loyalty card scheme. Having maximum fines or the right to erasure increase the chance that an individual chooses a loyalty card scheme the most.

Box 11 Interpretation of odds ratios

Estimates of the impact of the different rights on the choice between discount scenarios are expressed in odds ratios - the percentage change in the odds choosing one scenario (with the set of rights that come with it) over another.

Odds and probabilities are two ways of representing the likelihood of an event. The two measures are related with the *odds* of an option being chosen equal to the *probability* of an option being chosen divided by the probability of the other option being chosen:

$Odds = \frac{Probability}{1-Probability}$, or $Probability = \frac{Odds}{1+Odds}$.

Hence, a probability of 50%, for example, corresponds to odds of 1.

The odds ratio for a particular personal data right (or the existence of a maximum fine) is then defined as the odds of choosing a particular option when the data right exists divided by the odds of choosing the option if the data right does not exist, or (for any option x, and personal data right y):

$$odds\ ratio(y) = \frac{p(choosing\ x|y\ exists)/\left(1-p(choosing\ x|y\ exists)\right)}{p(choosing\ x|y\ does\ not\ exist)/\left(1-p(choosing\ x|y\ does\ not\ exist)\right)}.$$

The odds ratio for the discount is defined as the odds of choosing a particular option under a given discount divided by the odds under a discount of £1 less, or (for any option x):

$$odds\ ratio(discount) = \frac{p(choosing\ x|discount + £1)/(1-p(choosing\ x|discount + £1))}{p(choosing\ x|discount)/\left(1-p(choosing\ x|discount)\right)}.$$

[58] As compared with a situation where a particular right or a maximum fine does not exist.

Generally, an odds ratio of larger than 1 implies a positive impact of a personal data right or discount on the odds of choosing a particular option, while an odds ratio of smaller than 1 suggests that the data right or discount has a negative impact on the odds of an option being chosen.

A useful rule of thumb is that if the baseline probability of an event (an option being chosen) stands at 50% (corresponding to odds of 1), then an odds ratio of 1.50 suggests that a 50% increase in the odds of being chosen, or equivalently a 10 percentage point increase in the probability of being chosen. An odds ratio of 2.00 implies that there is a 17 percentage point uplift in the likelihood of being chosen, while an odds ratio of 2.50 implies a 21 percentage point uplift.

To aid interpretation of the previous and the following tables, we provide a guided example on how to interpret the results for the right to access for the loyalty card scheme. Interpretation of the other results follows the same pattern.

The coefficient for the right to access is 0.499, which is significant at any conventional significance level; the p-level is extremely small (< 0.1%). From this we may conclude that having the right to access positively impact the likelihood of someone choosing a particular loyalty card scheme. However, this coefficient cannot be interpreted in direct relation to probabilities. To do this, we ca can convert the coefficient into an odds ratio: $e^{0.499} = 1.647$. Hence, having the right to access increases the odds of choosing a loyalty card scheme by 64.7%. According to the rule of thumbs established in Box 11, this roughly corresponds an increase somewhat above 10 percentage points. One needs to be careful with this interpretation, however, since the conversion from odds ratios to percentage point increases is sensitive to the baseline probability. The rule of thumb is only correct of the baseline probability of choosing a loyalty card scheme is 50%. If the baseline is different, the rule of thumb merely gives an approximation.

The coefficient can also be converted into a pound figure for the willingness to pay for the right to access. As explained above, this is done by dividing the coefficient for the right to access with the coefficient for the discounts, $\frac{0.499}{0.129} \cong 3.86$. The logic behind this ratio is that it provides the discount required in the case the right to access is revoked to make someone equally likely to choose a loyalty card scheme, i.e. revoking the right to access has a negative 'impact' of 0.499 and the equivalent positive 'impact' of a discount is $0.129 * 3.86$. If the offered discount is higher, say £8, then a consumer is more likely to choose a loyalty card scheme with discount but without the right to access than without the discount and with the right to access. If the discount is lower, a consumer is less likely to choose a loyalty card scheme. Therefore, £3.86 is the required discount for a consumer to be willing to give up the right to access and still make the same choices as before.

A2.3.2 Smart meters

Table 5 provides the coefficient, p-values and odds ratios for the analysis of the probability of choosing a smart meter. As in the context of loyalty cards, all coefficients are positive and – with the exception of the right to data portability – highly significant. This shows that individuals are more likely to have a smart meter installed if they are granted to rights to access or erasure, if a maximum fine is in place or if the discount offered by having the smart meter installed is greater. The odds ratios show that the right to erasure and the existence of a maximum fine are the most important attributes in increasing the likelihood of choosing a particular smart meter.

Table 5 Impact of rights, fines and savings on the probability of choosing smart meter

	Coef.	P-value	Odds ratio
Right to request complete details of the personal data the provider has on you	0.357	<0.001	1.429
Right to copy or transfer your personal data from the current provider to another	0.117	0.158	1.125
Right to request the deletion or removal of personal data stored by the provider	0.831	<0.001	2.296
Provider faces a fine of £15m or 5% of turnover for non-compliance	1.022	<0.001	2.778
Saving you would achieve on average per month on your electricity bills	0.187	<0.001	1.206

Note: The coefficients of the conditional logit model by themselves are not easily interpretable. They tell us whether the inclusion of an attribute in any given choice increases (if significantly positive) or decreases (if significantly negative) the probability that an option is chosen. By taking the natural exponent of the coefficient, the odds ratios can be obtained. See Box 11 for further details on interpreting odds ratios.

Source: LE survey of consumers (2017) Choice experiment

A2.3.3 Health insurance voucher programme

Table 6 provides the coefficients, p-values and odds ratios of the analysis of the choices in this context. As in the previous two choice contexts, all coefficients are positive and highly significant, with the exception of the right to data portability. This confirms that most GDPR rights, the existence of a maximum fine and discounts impact the decision to take part in a voucher scheme. Again, the most important attributes, as indicated by the odds ratios, are the maximum fine and the right to erasure.

Table 6 Impact of rights, fines and discounts on the probability of choosing a health insurance voucher scheme

	Coef.	P-value	Odds ratio
Right to request complete details of the personal data the provider has on you	0.302	0.005	1.352
Right to copy or transfer your personal data from the current provider to another	0.033	0.744	1.034
Right to request the deletion or removal of personal data stored by the provider	0.703	<0.001	2.020
Provider faces a fine of £15m or 5% of turnover for non-compliance	0.920	<0.001	2.508
Value of reward vouchers you would receive on average per month	0.118	<0.001	1.125

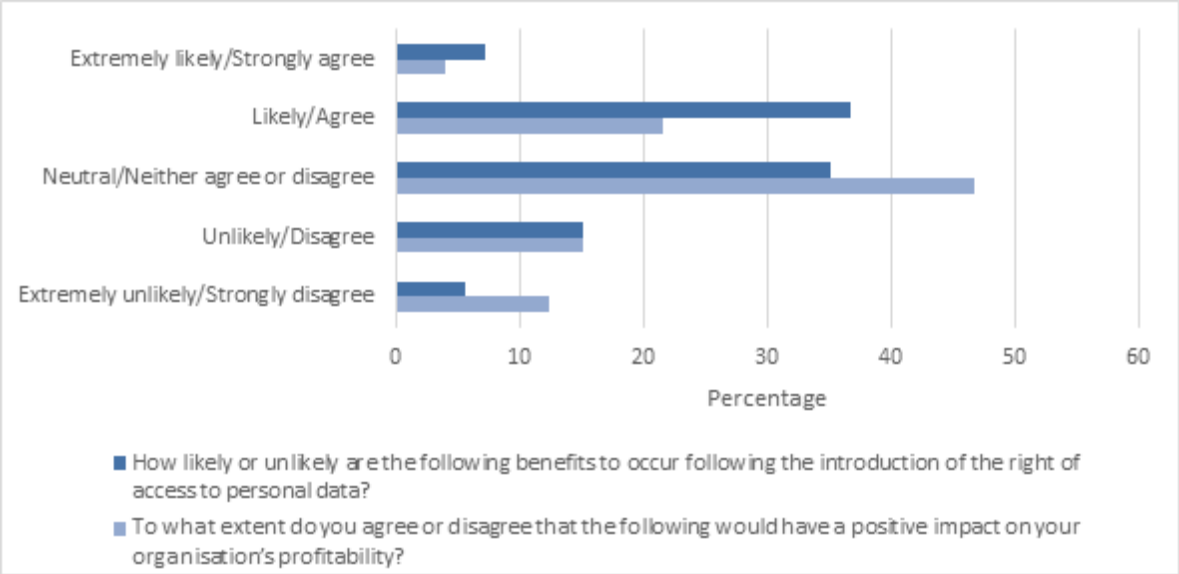
Note: The coefficients of the conditional logit model by themselves are not easily interpretable. They tell us whether the inclusion of an attribute in any given choice increases (if significantly positive) or decreases (if significantly negative) the probability that an option is chosen. By taking the natural exponent of the coefficient, the odds ratios can be obtained. See Box 11 for further details on interpreting odds ratios.

Source: LE survey of consumers (2017) Choice experiment

Annex 3 Professionals survey results

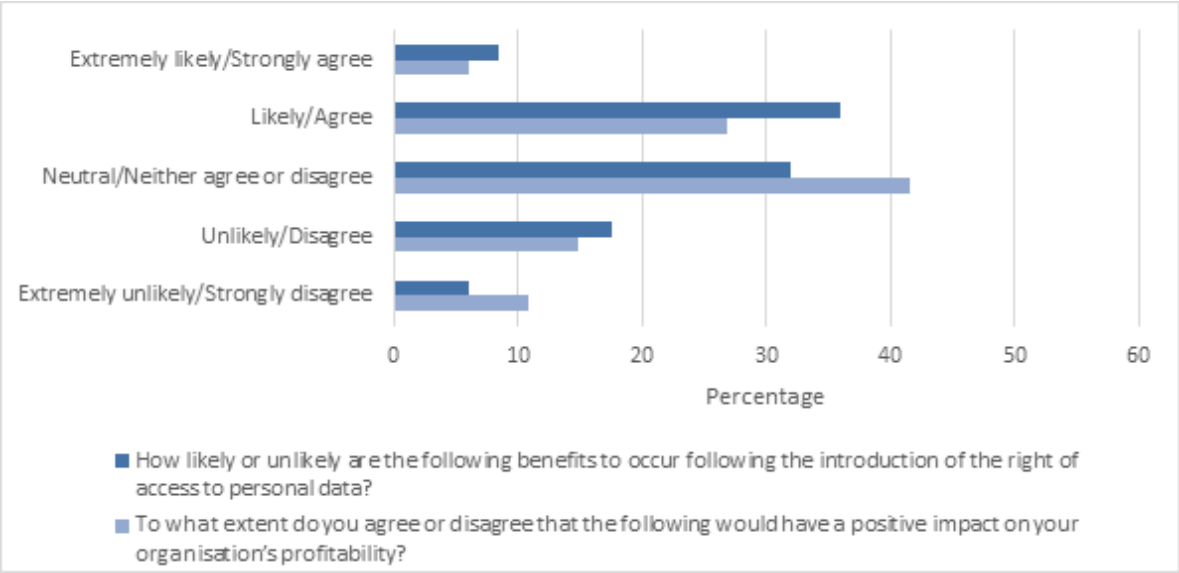
A3.1 Right of access

Figure 58 Access requests as warning to companies



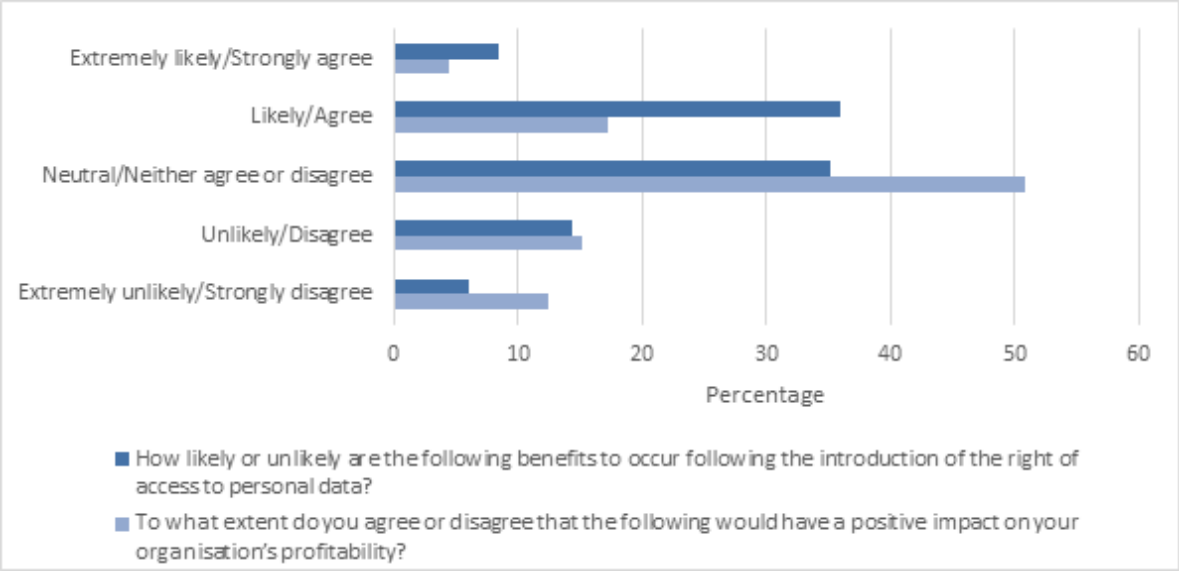
Source: LE survey of data protection professionals (2017)

Figure 59 More accurate data



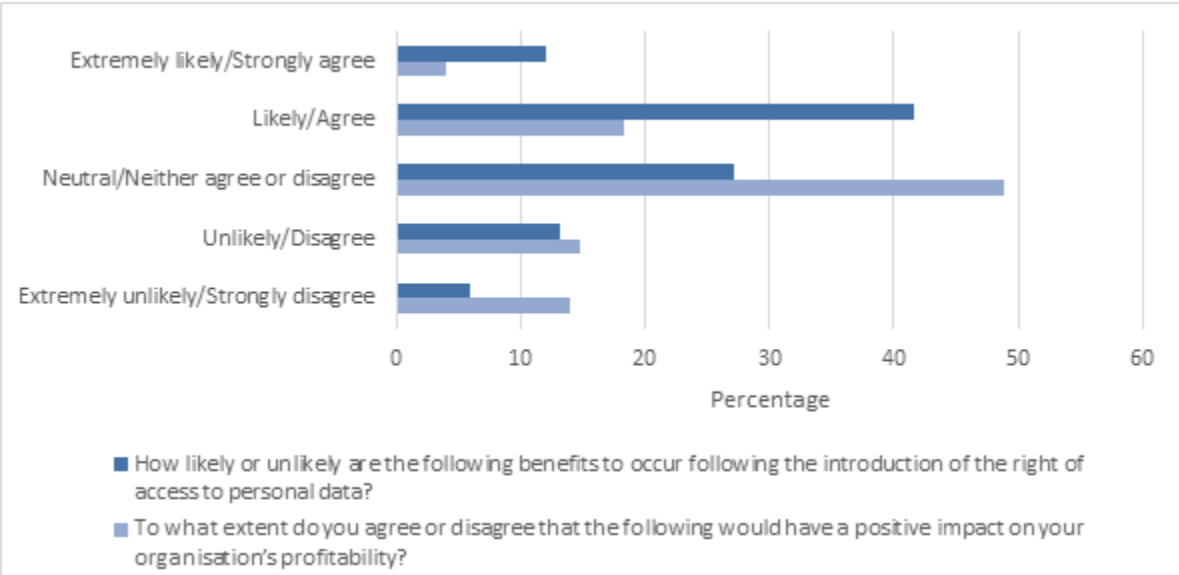
Source: LE survey of data protection professionals (2017)

Figure 60 Greater security through greater scrutiny



Source: LE survey of data protection professionals (2017)

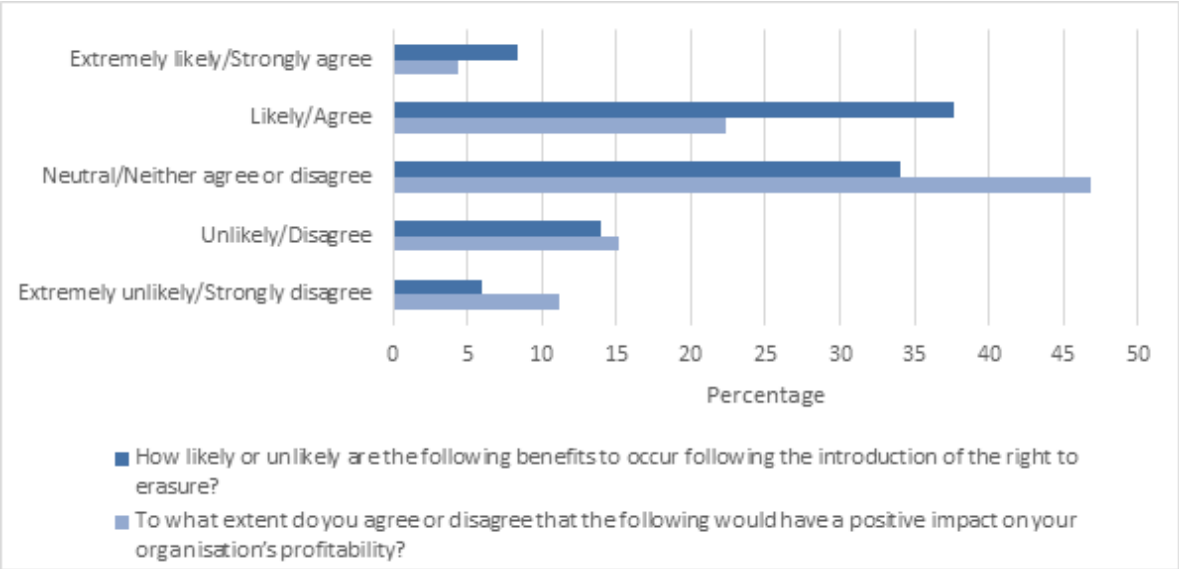
Figure 61 Greater consumer control



Source: LE survey of data protection professionals (2017)

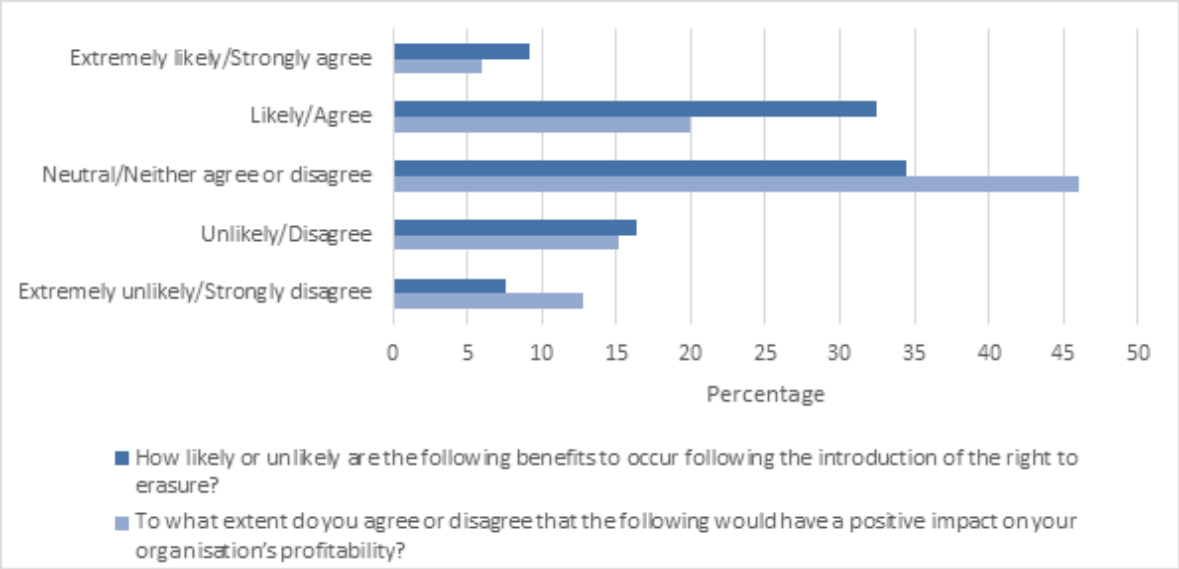
A3.2 Right to erasure

Figure 62 Erasure requests as warning sign to companies



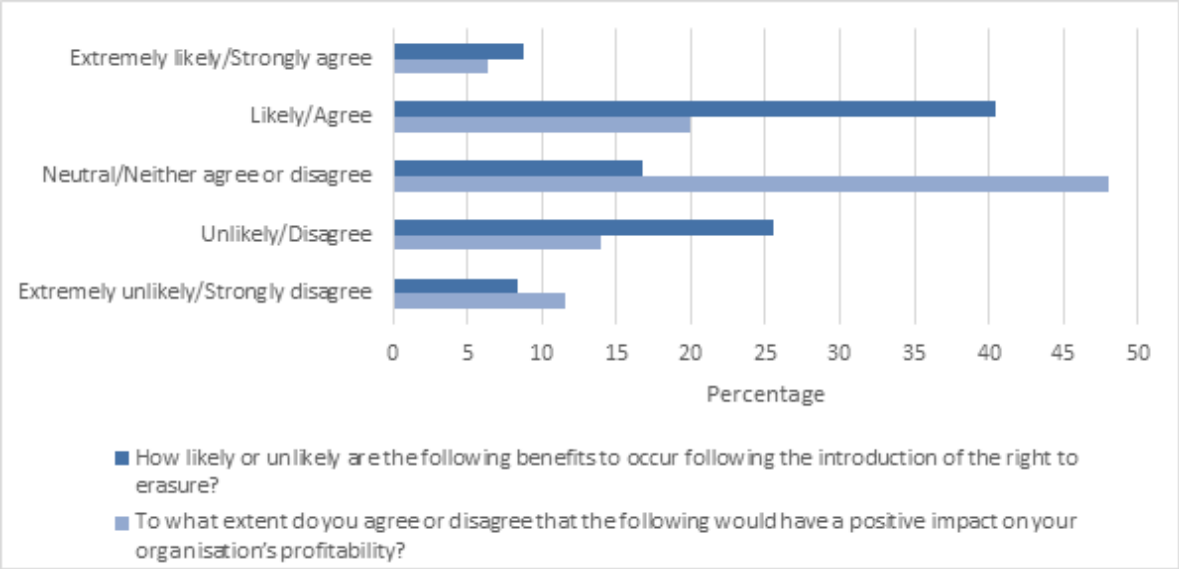
Source: LE survey of data protection professionals (2017)

Figure 63 Erasure requests as punishment to firms that have lost consumer trust



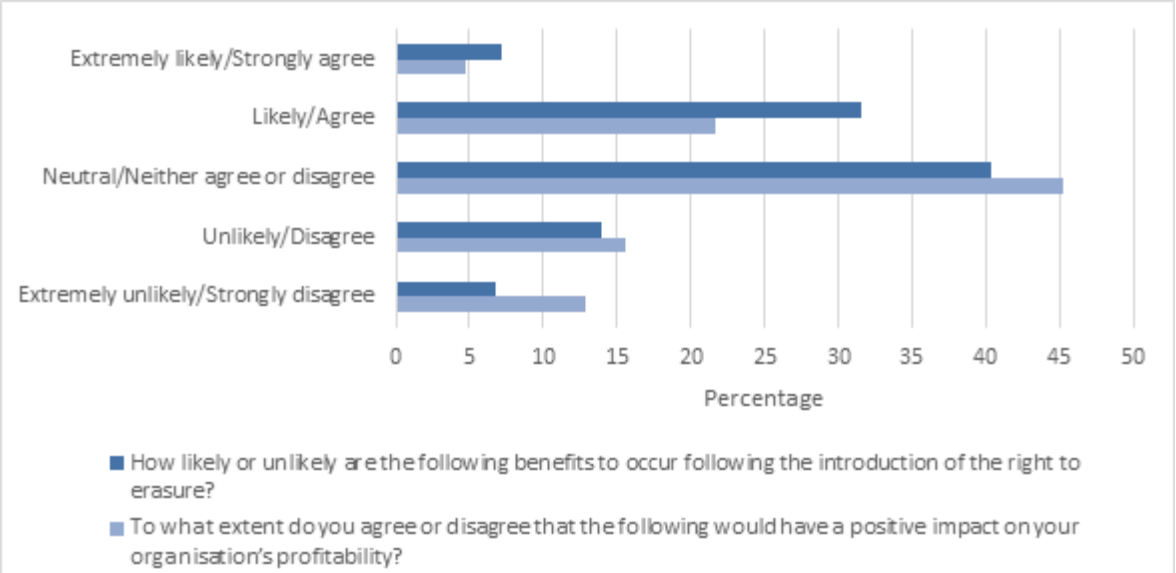
Source: LE survey of data protection professionals (2017)

Figure 64 Ending harmful use of personal data



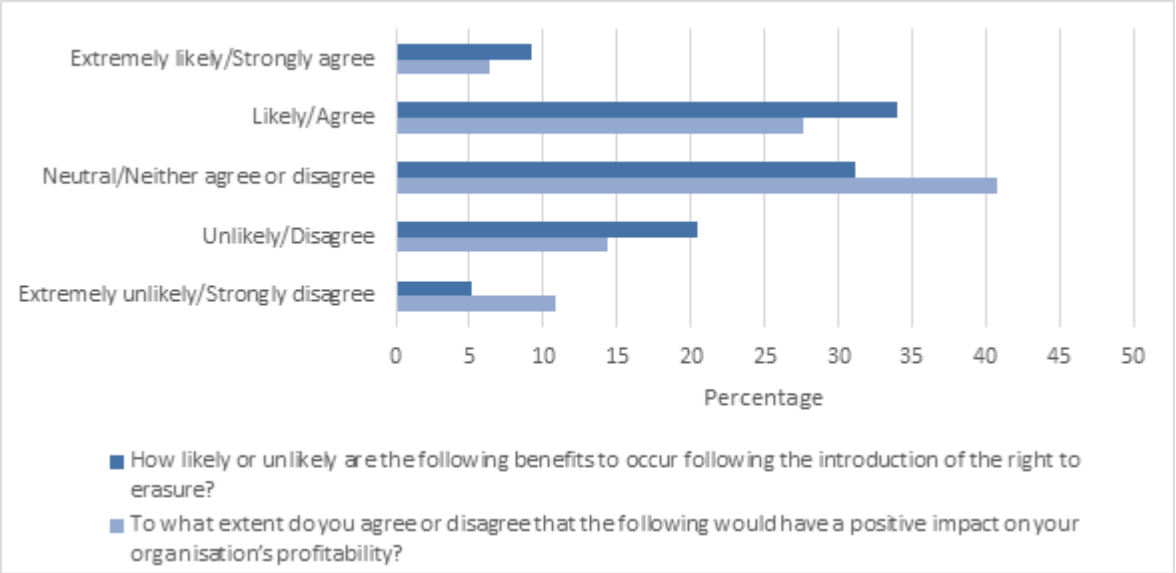
Source: LE survey of data protection professionals (2017)

Figure 65 Consumers more likely to try new, data-intensive services



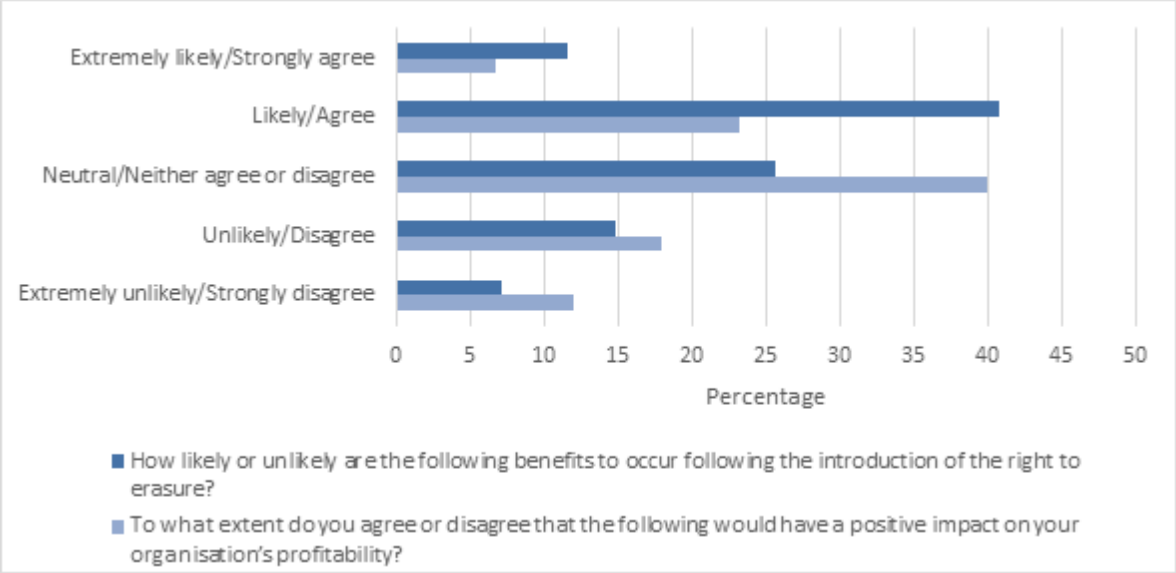
Source: LE survey of data protection professionals (2017)

Figure 66 More accurate data



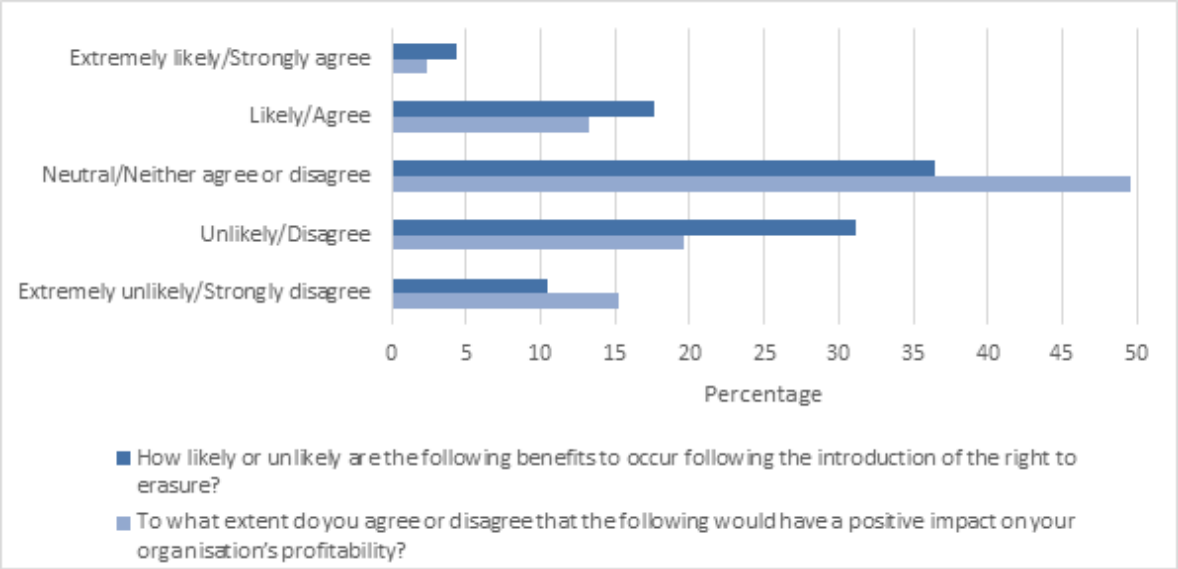
Source: LE survey of data protection professionals (2017)

Figure 67 Greater consumer control



Source: LE survey of data protection professionals (2017)

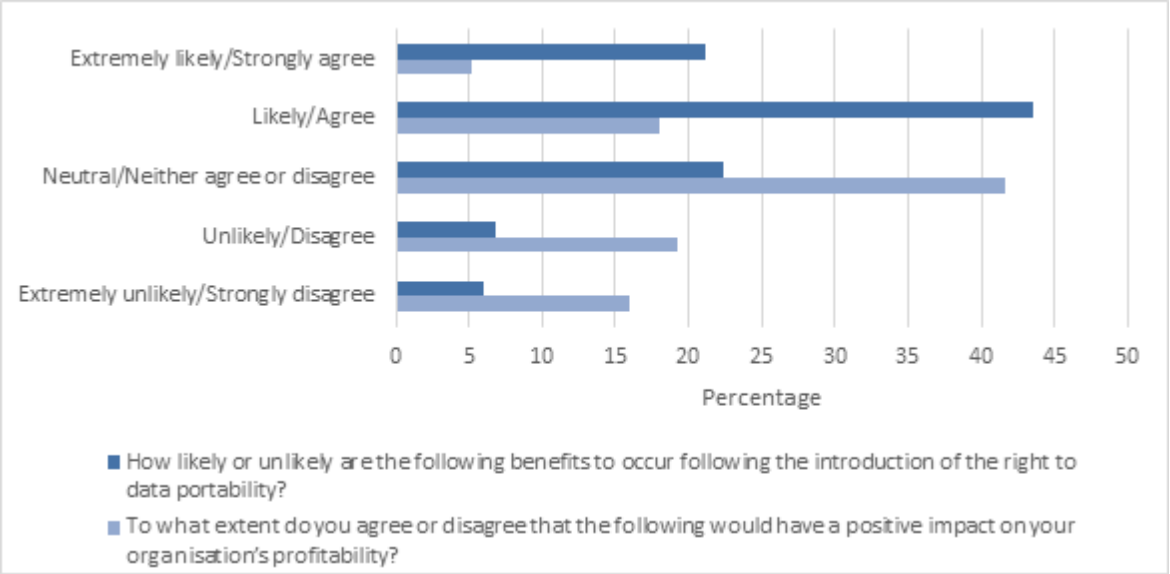
Figure 68 Consumer cost saving due to dealing with one data controller only



Source: LE survey of data protection professionals (2017)

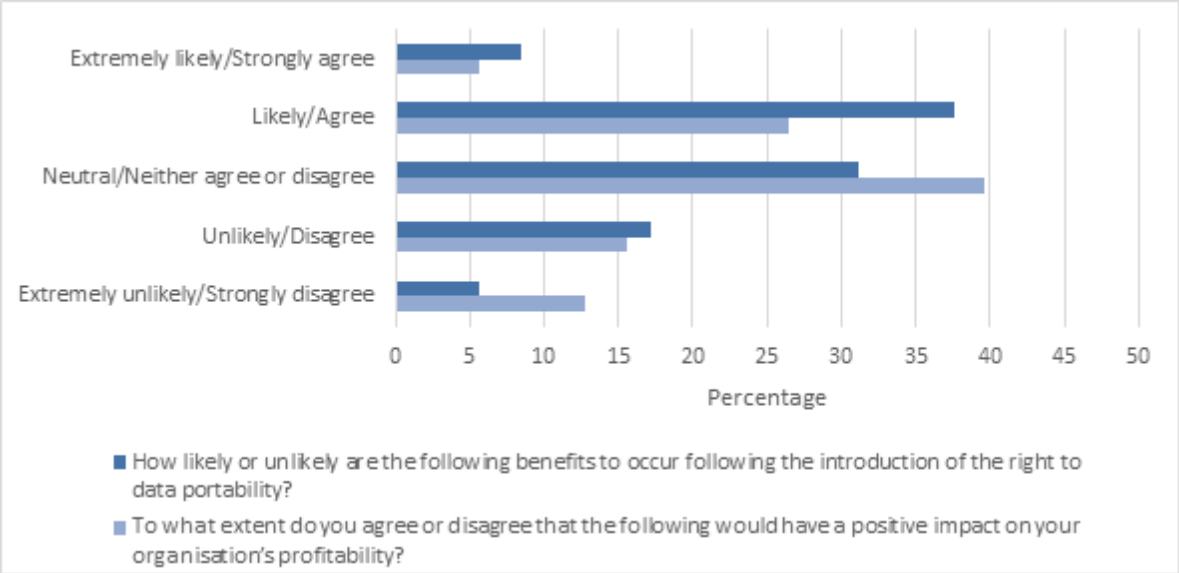
A3.3 Right to data portability

Figure 69 Secondary market for customer data



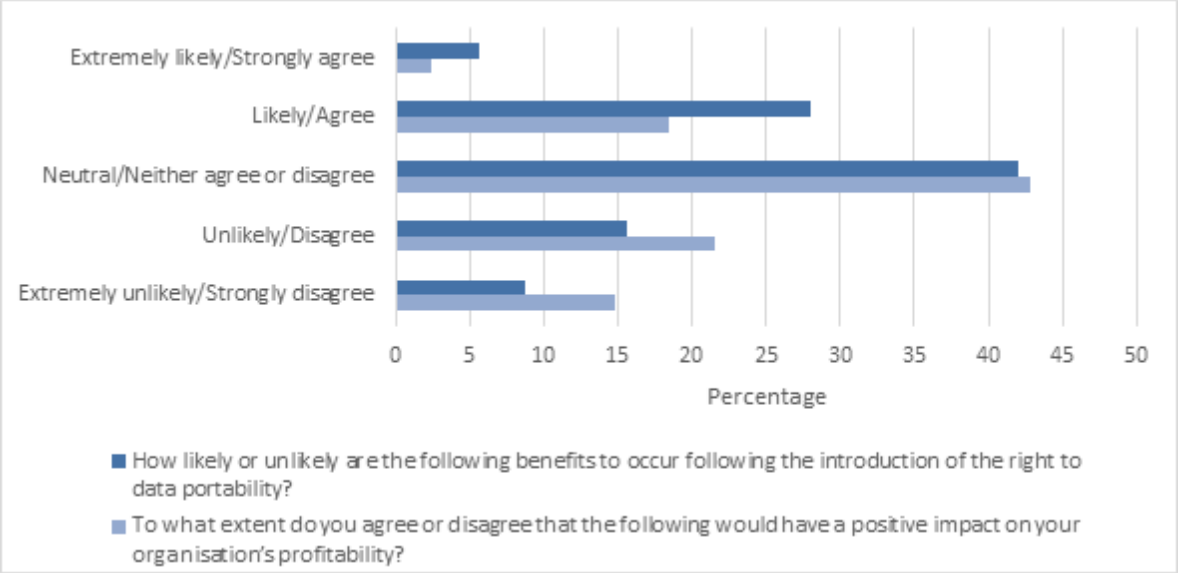
Source: LE survey of data protection professionals (2017)

Figure 70 Reduced costs to due access to pre-existing data



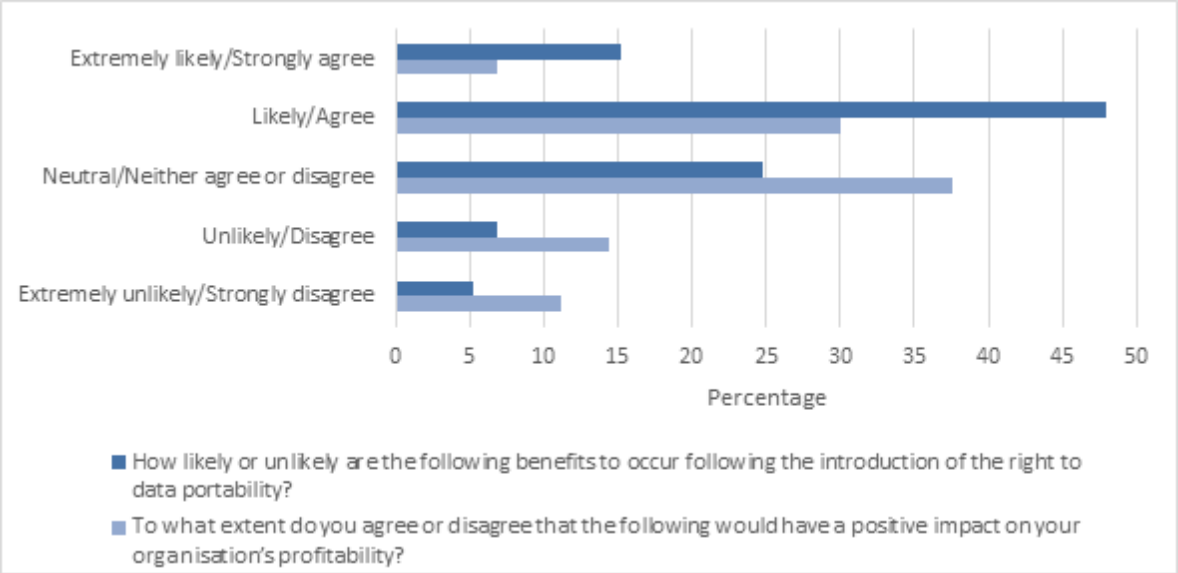
Source: LE survey of data protection professionals (2017)

Figure 71 More competition among providers



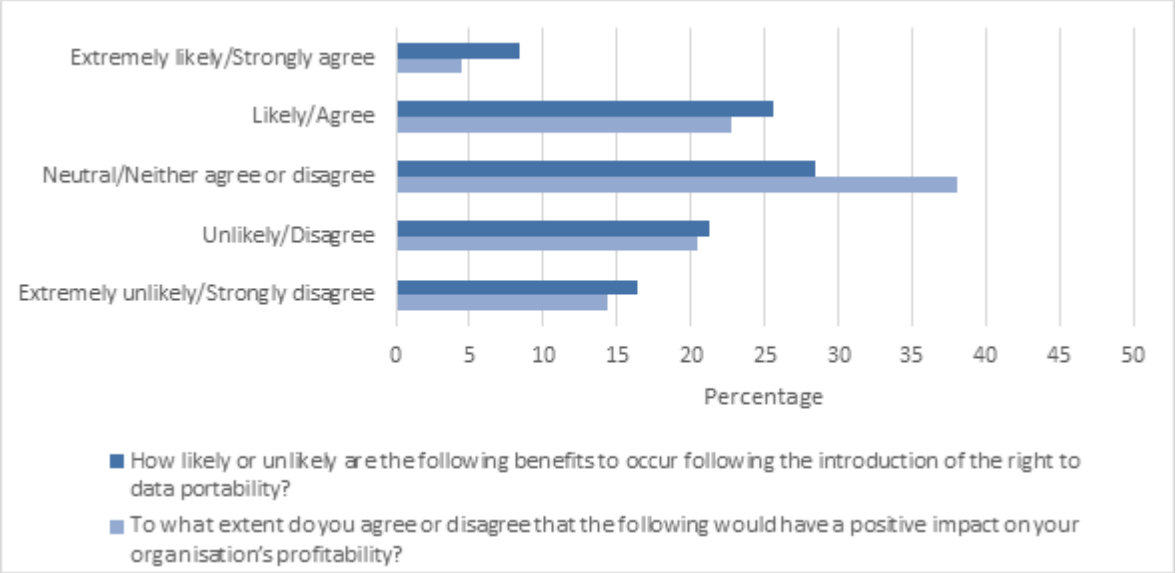
Source: LE survey of data protection professionals (2017)

Figure 72 Time savings for consumers



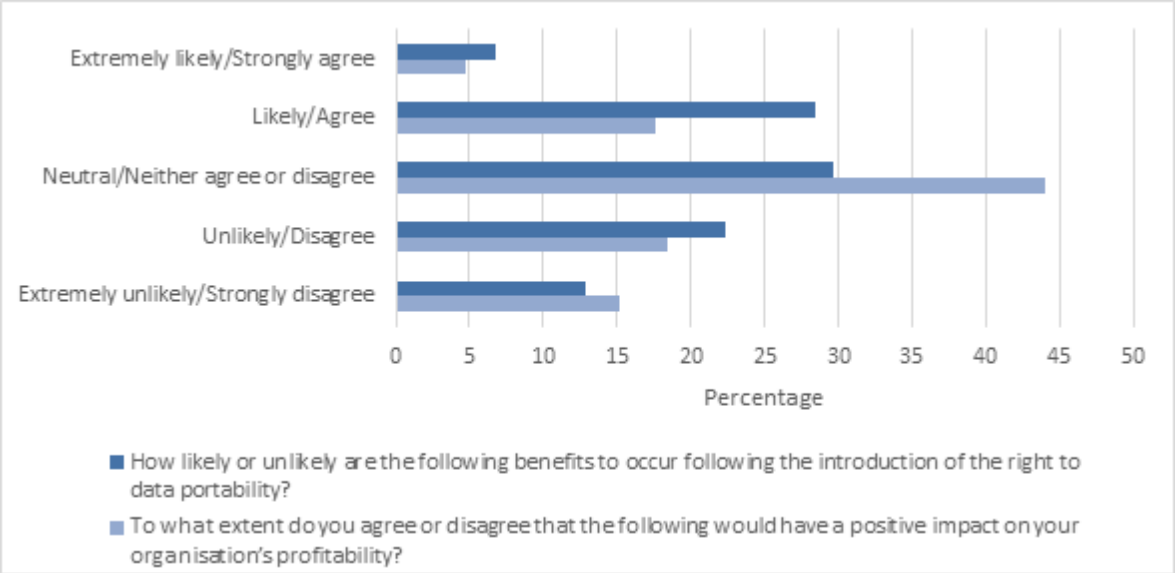
Source: LE survey of data protection professionals (2017)

Figure 73 Greater consumer control over own data



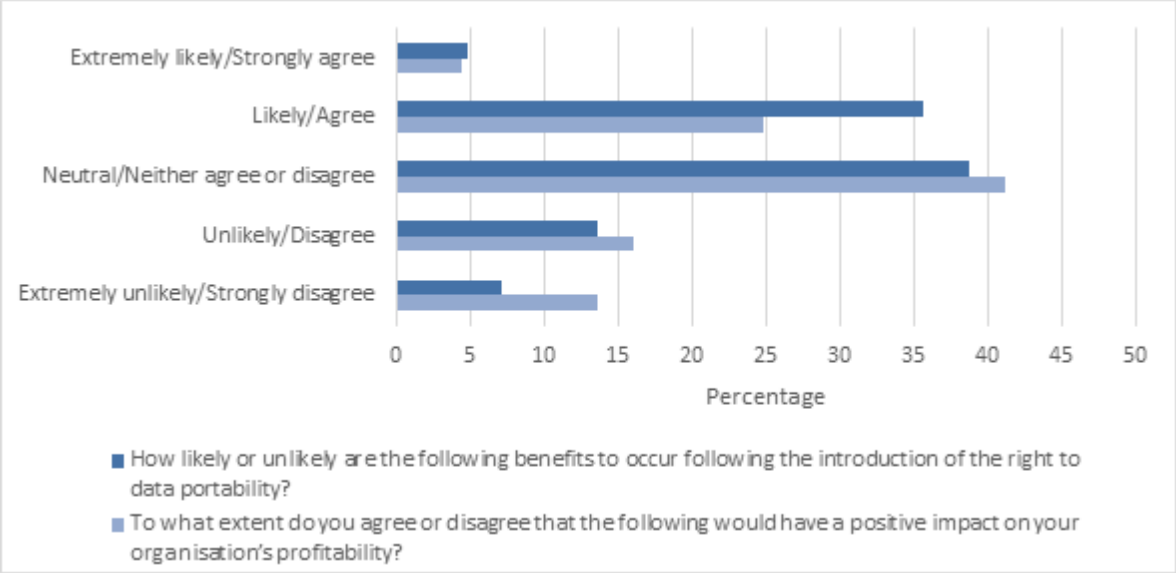
Source: LE survey of data protection professionals (2017)

Figure 74 Ability to do own analysis



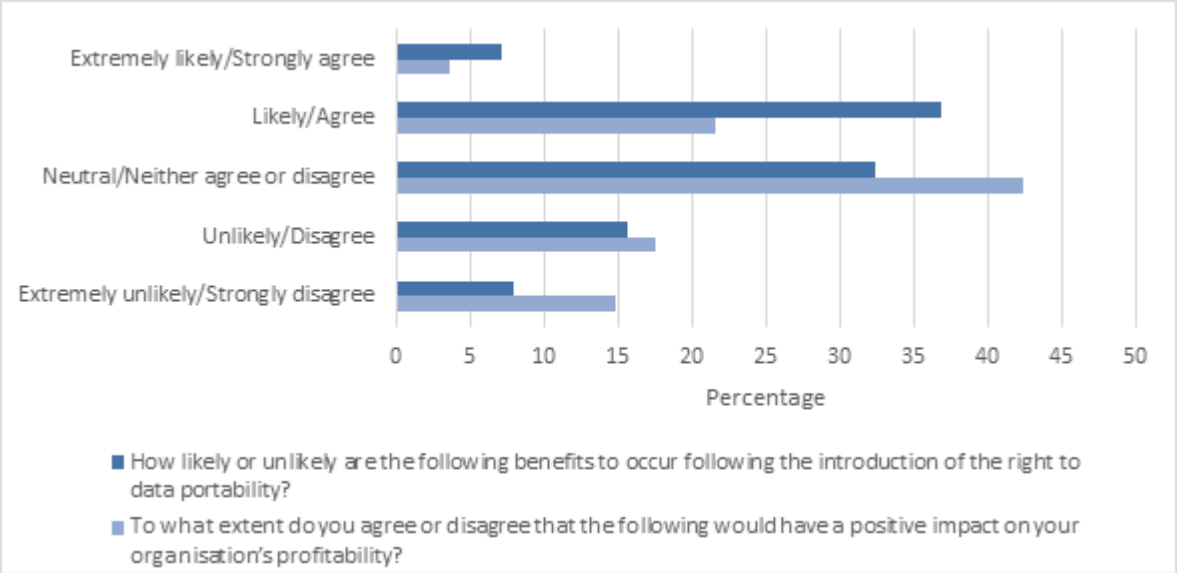
Source: LE survey of data protection professionals (2017)

Figure 75 Better or more tailored services



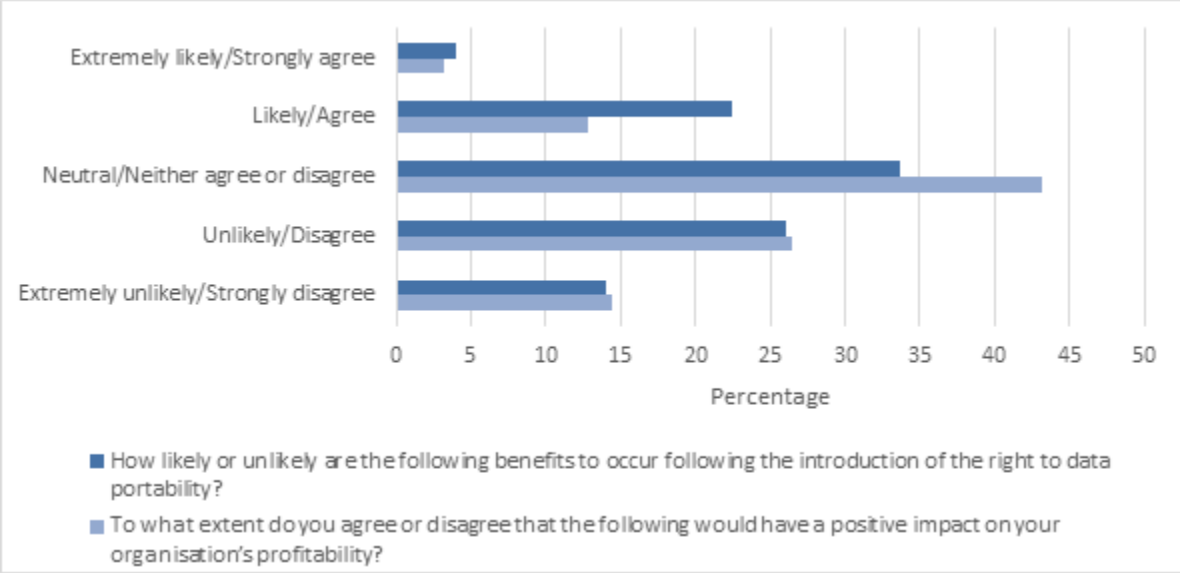
Source: LE survey of data protection professionals (2017)

Figure 76 Personalised pricing based on past usage



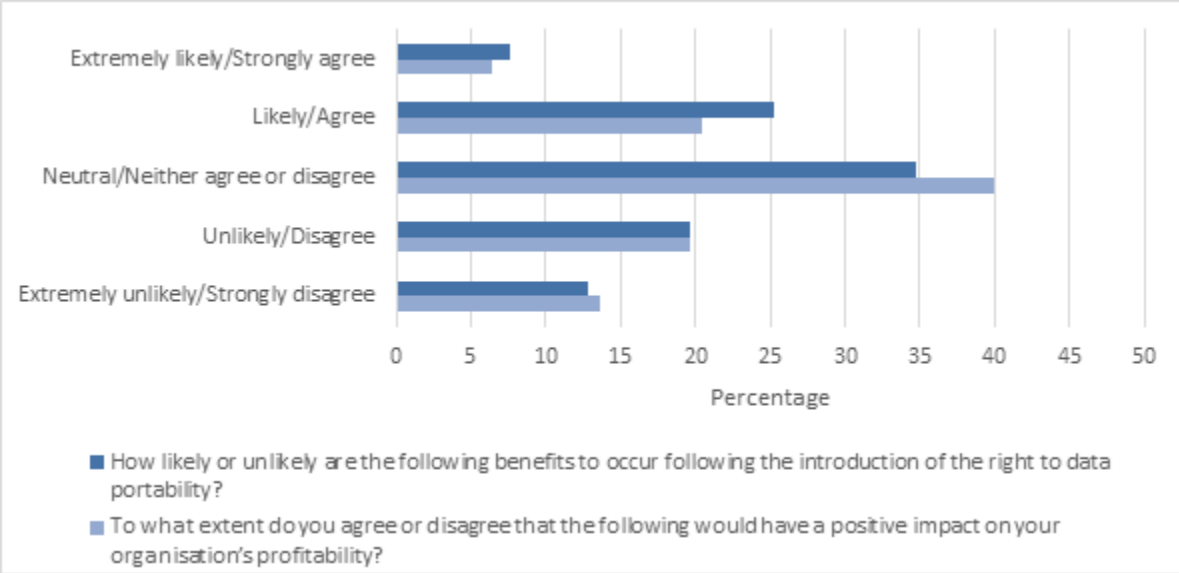
Source: LE survey of data protection professionals (2017)

Figure 77 Cheaper prices due to receiving pre-existing data



Source: LE survey of data protection professionals (2017)

Figure 78 Protection against data loss



Source: LE survey of data protection professionals (2017)

Annex 4 Benefits of consumer switching

Making it easier for consumers to shift their custom from one supplier to another is a potential source of substantial consumer benefit, directly through the ability of consumers to access better deals by switching, and indirectly, through a more competitive market in which the constant threat of switching ensures that prices and service levels converge to the optimal level from the consumer perspective. Pricing of products and services that involve the disclosure of substantial amounts of personal data is often complex (utilities, financial services) and may involve trade-offs between disclosure and access to 'free' services (social networks) or discounts (online shopping, loyalty schemes).

A4.1 Switching as a source of benefit

Shopping around for deals in those contexts is a complex task, and the mental effort to evaluate them is significant. A vast amount of literature from economics and psychology has shown that the fully rational consumer framework is limited in its ability to describe actual consumer behaviour.[59]

Consumers' cognitive capacities are in fact often limited which turns the fully rational choice setting into a rather unrealistic starting point. Instead, it is more sensible to assume that individuals are **boundedly rational**[60] which can affect their decision making at all stages of their purchasing journey. This means that contrary to the fully rational model, individuals' cognitive capacities or their resources (e.g. time) dedicated to the choice at hand are limited.

Such boundedly rational behaviour can be observed in the form of **biases** that deviate from the fully rational benchmark. Behavioural economics offers several explanations to the most common among these biased behaviours. The following biases are present in many markets that are 'personal data intensive', notably financial services and utilities markets:

- **Status quo bias (a.k.a endowment effect, default bias):** It is commonly found that individuals do not actively shop around for new deals and that, once chosen, they tend to remain with a certain provider although alternative deals may be more advantageous. Both behaviours can be explained through the status quo bias which is the tendency to stick to one's endowment or default.[61]
- **Loss aversion: The** status quo bias is directly linked to loss aversion. Kahneman and Tversky (1979) showed that individuals **dislike losses** much more than they appreciate equally sized gains. In switching from one supplier to another, individuals are giving up, hence losing, their current deal. In order to compensate for this loss, the new deal must yield disproportionately high advantages, otherwise, loss averse consumers may not find it worthwhile to engage in switching and stick to their current deal, i.e. the status quo.
- **Availability heuristic:** In order to **simplify** the complex choice of which provider and deal to choose, the availability heuristic leads individuals to focus on **information which is**

[59] See for example: Kahnemann (2003) 'Maps of Bounded Rationality: Psychology for Behavioral Economics', American Economic Review. Thaler (1990) 'Anomalies: Saving, Fungibility, and Mental Accounts', Journal of Economic Perspectives; Thaler (1991) 'Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias', Journal of Economic Perspectives.

[60] Simon (1955) "A Behavioral Model of Rational Choice." Quarterly Journal of Economics.

[61] Knetsch (1989) 'The endowment effect and evidence of nonreversible indifference curves'; Kahneman, Knetsch and Thaler (1991) 'Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias'.

readily available and currently important to them.[62] This can result in biased access and assessment of information since not all information is given equal attention. This bias is particularly acute in cases where user data can yield advantageous insights, but is not accessed or used in the decision-making process.

- **Present bias:** Individuals tend to be **present biased,** meaning that they focus excessively on the present and fail to appreciate events happening in the future.[63] This bias delivers an additional explanation as to why consumers tend not to switch providers. They may focus excessively on the switching costs (i.e. time, effort or payment of exit fees) and underappreciate the long term savings they may realise from switching. Reducing the cost of switching through data portability directly counteracts this bias.
- **Narrow framing:** The literature speaks of narrow framing when individuals have trouble seeing the bigger picture as a result of numerous single events.[64] In the context of energy billing, for example, this may lead consumers to having difficulties integrating monthly or quarterly energy consumption into annual figures and vice versa. Again, making use of historical data can mitigate this problem.

A4.2 Evidence on the benefits of switching from the electricity and current account markets

Certain retail markets, notably for electricity, financial services and telecoms, have been investigated because of the potentially large benefits from switching available to consumers, which contrasts with a very low observed incidence of switching. These markets offer useful insights into the potential benefits available as a result of data portability more broadly.

However, electricity supply and to a lesser extent current accounts and mobile phones are exclusive contracts in the sense that switching providers usually involves terminating the relationship with one and commencing the relationship with another. In many settings, consumers maintain relationships with different providers in parallel (it is common that households are members of different, loyalty schemes), which is likley to dilute the benefits from switching.

What is clear, however, that consumers in many markets show too much loyalty to providers of goods and services in the sense that they would benefit financially from switching more frequently. Below we provide two example calculations to illustrate the scale of potential benefits.

A4.2.1 Electricity market

The first market analysed is the market for electricity. The European Commission has commissioned research into the functioning of the European electricity markets (European Commission, 2015). Part of that research focused on switching costs and behaviour, which will be used here. The analysis of benefits to consumer switching and potential additional value generated by data portability is built up in steps outlined below. We focus on UK benefits only.

The Commission's report provides data on potential benefits for switching per consumer. Particularly, it provides three consumer profiles – low, medium and high consumption pattern – and

[62] Tversky, Amos; Kahneman, Daniel (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*.

[63] Laibson (1997). Golden eggs and hyperbolic discounting. *The Quarterly Journal of Economics.*

[64] Thaler, Tversky, Kahneman, Schwartz (1997). The effect of myopia and loss aversion on risk taking: an experimental test. *The Quarterly Journal of Economics.*

provides for each of these the spread between the cheapest, the average and the highest tariff obtained in a mystery shopping exercise.

The relevant data for the UK can be found the table below. This also provides the assumed consumption for each profile.

Table 7 Tariff dispersion per consumption profile

Profile	Assumed kWh	Lowest tariff	Average tariff	Highest tariff
Low consumption	1,000	€0.18/kWh	€0.21/kWh	€0.26/kWh
Medium consumption	3,500	€0.14/kWh	€0.15/kWh	€0.18/kWh
High consumption	10,000	€0.11/kWh	€0.14/kWh	€0.18/kWh

Note: Assumed kWh is the assumed consumption of electricity for each of the consumption profiles.

Source: EC (2015)

These figures can be used to generate a per-consumer benefit of switching. An average consumer benefit can be calculated by applying $assumed\ kWh * (average\ tariff - lowest\ tariff)$. An upper bound consumer benefit can be calculated by applying $assumed\ kWh * (highest\ tariff - lowest\ tariff)$. Both calculations assume that consumer benefit only comes from lower prices – not taking into for instance the energy mix – and the upper bound calculation assumes that all consumers are paying the highest possible tariff. Calculations are provided in below.

Table 8 Consumer benefits to switching

Profile	Average consumer benefits	Upper bound consumer benefits
Low consumption	€30	€80
Medium consumption	€35	€140
High consumption	€300	€700

Source: LE based on EC (2015)

The Commission's report shows that 48% of households changed either electricity supplier or tariff with the same supplier in the three years prior to data collection. At 27,037,400 households in 2016 (Office for National Statistics, 2016), this represents 12,977,952 households.

The total number of switchers can be multiplied out by per consumer benefits to generate total consumer benefits achieved in switching. This is provided in Table 9 per consumption profile[65]. By multiplying out average benefits with the number of affected household, we implicitly assume that each household has the same consumption profile. Given that we do not how different often different consumer profiles occur in real-life, this calculation can only give a rough indication of consumer benefits.

Table 9 Total consumer benefit, in Pounds

Profile	Total average consumer benefits	Total upper bound consumer benefits
Low consumption	£282.6 million	£753.6 million
Medium consumption	£329.7 million	£1,318.8 million
High consumption	£2,826.0 million	£6,594.0 million

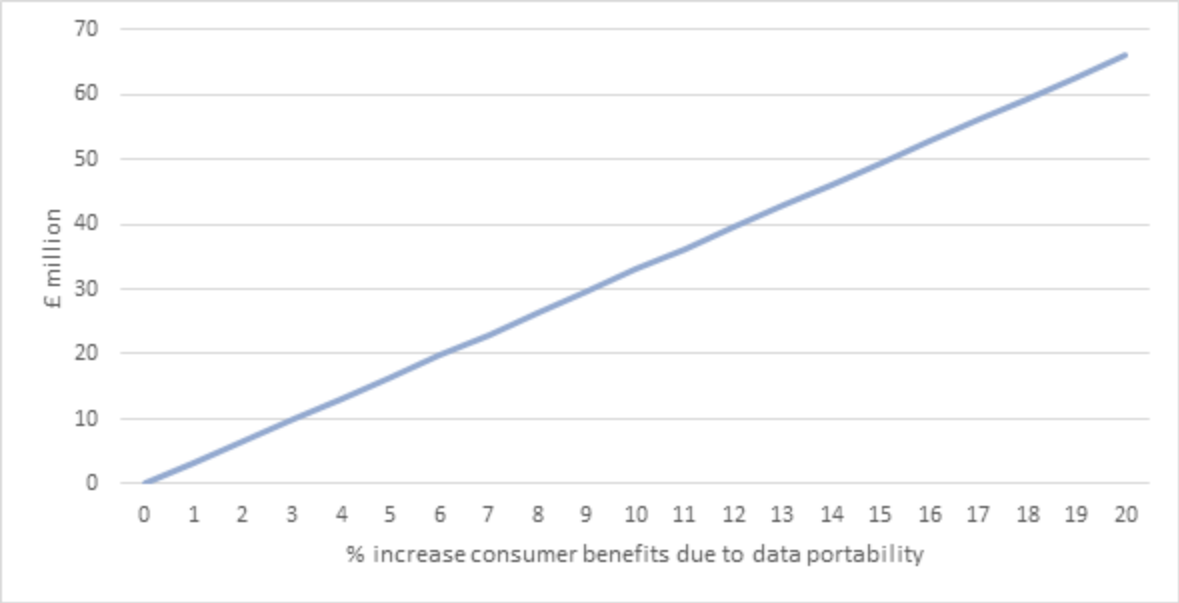
Source: LE based on EC (2015)

[65] £0.72584 to €1. Average conversion rate over 2015 provided by Eurostat (ert_bil_eur_a).

Additional consumer benefits from Data Portability

There is no data on the additional consumer benefits which arise from the right to data portability. However, one can expect that data portability decreases switching costs and therefore should increase switching itself. Given that no appropriate data exists, Figure 79 plots different values which may give a range of the total benefits from switching in the electricity market that flow from data portability. Figure 79 only presents additional profits calculated from the total average consumer benefits, as these are more likely to be close to the truth. Effectively, it plots $total\ consumer\ benefit * percentage\ increase\ of\ benefits\ from\ data\ portability$ for different, hypothetical, percentages.

Figure 79 Possible additional values to consumer benefits from consumer switching enabled by data portability (medium consumption case)



Note: the range chosen for additional benefits from data portability is pure conjecture and not based on data.

Source: LE based on EC (2015)

This suggests that, from 2015 data, additional benefits arising from easier switching due to data portability are most likely to be around £50 million.

A4.2.2 Current Account market

The second market analysed for consumer benefits to switching is the UK market for current accounts. The Current Account Switch Service (CASS) was introduced in September 2013, aimed at making current account simpler and quicker (Financial Conduct Authority, 2015). CASS fullfills a similar role as data portability would do in the case of current accounts. It transfers direct debits and account information from one bank to another. The same thing can also be operationalised through mandatory data portability. Therefore, it is reasonable to take consumer benefits arising from current account switching through CASS as a proxy of potential consumer benefits arising from switching through data portability.

As for the electricity market analysis, the first step is to calculate the average individual benefits to switching. The Competition and Market Authority conducted a study of the retail banking sector

(Competition and Market Authority, 2015). It found that, by switching to the cheapest current account, the average consumer would save £70 a year, people with an overdraft would save £140 a year and heavy users of overdrafts would save £260 a year.

The second step is to figure out how many more current accounts have been switched since the introduction of CASS relative to the a counter-factual in which CASS does not exist. One simple way of looking at this is to compare year-on-year the number of current account switches through CASS and its predeccesor.

The Financial Conduct Authority (2015) shows that the number of current account switches through CASS increased by 22% to 1.2 million in the year after introduction, as compared to the number of switches through the predeccesor system. However, the number switches decreased to only 16% more than previously a couple of months later. Furthermore, the number of switches is only 2% higher than the peak number of current account switches under the old system. These number can provides us with a low, medium and high estimate for additional current account switches due to a simplified system.Table 10 takes these percentage and converts them into a level increase of current account switches based on 1.2 million switches with CASS[66].

Table 10 Number of additional switches due to CASS

Estimated increase of current account switches due to easier switching	Number of additional current accounts switched
Low estimate (2%)	19,672
Medium estimate (16%)	157,377
High estimate (22%)	216,393

Note: Level values have been rounded to the nearest integer.

Source: LE based on FCA (2015)

Multiplying out these level increases with average consumer benefits obtained previously provides the estimate of consumer benefits generated by CASS (and hence our proxy for data portability). This is provided in Table 11. This table assumes that all current account users are of a single type.

Table 11 Consumer benefits due to CASS

Estimate impact CASS	Average user	Overdraft user	Heavy overdraft user
Low estimate (2%)	£1.4 million	£2.8 million	£5.1 million
Medium estimate (16%)	£11.0 million	£22.0 million	£40.9 million
High estimate (22%)	£15.1 million	£30.3 million	£56.3 million

Source: LE based on FCA (2015) and CMA (2015)

A4.2.3 Mobile phone numbers

For phone number portability (in the US), Park (2011)[67] finds that in the mobile phone market prices decreased between 0.97% and 6.81% after the introduction of number portability (which is not technically data portability, but related). The total drop depends on the volume of the calls. People with high call volume benefit more.

[66] Given that the 1.2 million is the number after CASS was introduced and represents 22% higher yearly switching volume, the calculation applied in the table is as follows: $(1.2\ million/1.22) * (estimate/100)$.

[67] http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6451.2011.00471.x/full

Annex 5 Online forum transcripts

This annex provides the transcripts of the forums verbatim.

A5.1 Forum 1: general GDPR rights (06-10 March 2017)

A5.1.1 Day 1: Introductions and Rights to Data Portability

- Welcome to the forum! Please introduce yourself with your first name only, role and sector you work in. What are your data protection responsibilities in your organisation?
- What comes to mind when you think about 'data protection'? Please describe any word associations, images, feelings, examples that come to mind. Please upload any images, text or film to help demonstrate your opinions.
- Are you aware of the General Data Protection Regulation (GDPR)? If so, how are you aware of it? What comes to mind when you think about the GDPR? (E.g. its role, strengths/ weaknesses and perceived benefits)?

Each day over the next 4 days, we will introduce a key component of the regulation and ask you for your feedback on expected impacts on your business and customers/ clients etc. (Please note this means that today's questions may take a little longer to complete than the rest of this week's!) **To start- please read the information below on the right to data portability...**

'The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. (ICO)'

- Overall, do you envisage the right to 'data portability' to result in tangible benefits for your organisation?
- Do you envisage the right to 'data portability' to lead to any changes in consumer behaviour? Why or why not? If so, what type of changes do you expect?
- Can you imagine this right providing any benefits to customers and/or your organisation? Why or why not? Please explain what you can imagine the benefits being.
- **Below is a list of 6 potential benefits**- please explain if you agree or disagree with each potential benefit and <u>why you think this</u>:

1) Time savings for individuals providing data to your organisation
2) Greater opportunity for your organisation to acquire and use more detailed data on individuals providing data to your organisation
3) Greater opportunity to use more / more detailed data on individuals to improve the service provided by your organisation?
4) Cost savings for your organisation (e.g. reduced need to collect data from new users)
5) Greater opportunity for a secondary market for data (e.g. 3rd party services, analysis, switching services)
6) Increase competition in the market your organisation operates in

Posted by Paul M on 06 Mar 2017 10:34 AM

My name is Paul, I am Operations Director of a small firm in financial services media, publishing and research. We are sometimes granted access to financial services firms' databases. I have data protection responsibilities in line with the other directors.

Data protection is absolutely key- it is not an onerous responsibility. It is something all firms should pay close attention to. I am aware of GDPR- it is something that should be respected by all businesses.

I am not sure that data portability will have any specific benefits for us, although it will help in the consistency of information that people are expected to give. In terms of consumer behaviour, it will hopefully lead to more people understanding what information to provide and what information not to provide to third parties.

In terms of the 6 potential benefits listed:-

1) Yes- it should help here, slightly.
2) I am not sure yet whether data will be more detailed, but it should eb more accurate/ consistent.
3) Yes, slightly.
4) Yes, definitely. Databases are often inconsistent/ incomplete- this should help.
5) Yes, if data collected is more consistent.
6) I am not sure at this stage.

Posted by Rhiannon R on 06 Mar 2017 5:33 PM

Hi Paul,

Thanks very much for your comments.

I'm interested in your thoughts on a potentially greater opportunity for a secondary market for data.

If data collected is consistent enough to allow for this, what do you think the main developments will be? What sort of effect might this have on your firm, if any? Would it have much effect on you as a consumer?

Thanks,
Rhiannon

Posted by Paul M on 07 Mar 2017 7:06 PM

Hi Rhiannon,

Thanks for this.

I am not sure that our firm will benefit from this, although the potential benefits to marketers and consumers generally seems huge. The market for secondary data could become the 'new geodemographics' if data is consistent. However, it is a big 'if.' Geodemographics is based on census data, this would not be so from the outset there would be some holes.

I hope this is helpful.

Many thanks,

Paul

Posted by Sallie T on 06 Mar 2017 2:46 PM

My name is Sallie, I am the Operations Director for a SME dealing in insured repairs for IT & mobile telephony equipment on behalf of personal lines insurers and for the extended warranty/service guarantee market. Our business is 90% B2B with very little direct customer contact. I am aware of GDPR.

While we collect very little personal data to facilitate our repair processes, data security forms a critical part of my role because of the nature of what we repair: laptops, mobile phones, tablets etc. Most items arrive containing quantities of the customer's own personal data and while this is not accessed during our repair process, the burden of maintaining data security during that process falls to us and something which calls for high levels of physical security, in depth pre-employment screening and a very robust set of data security standards, protocols and procedures. As a result data protection is always at the forefront of my mind and that of our business clients. We would all like to see greater levels of consumer awareness and ownership for their own data particularly with the advent of cloud storage and devices locked to it and I fear this issue is only going to get worse over time. Without doubt data protection/security is a massive and costly responsibility for my company.

Data portability will have very little impact or benefit as we collect very limited amounts of data and each instance of data collection is a one-off event following an insured incident or equipment malfunction with little likelihood of repetition, ongoing relationship or cross-over in terms of provision of further services.

Due to the nature of our business and business model I can't envisage much, if any, change in consumer behaviour with regard to our business as the contact they have with the company is the end stage in an insurance claim, so I would envisage data re-use to be restricted to occasions when claim history is needed by the customer for their own insurance purposes.

The customer may benefit from convenience in terms of speed and ease of provision of data but I think overall, the biggest benefit would be for a future recipient of ported data which could potentially be more accurate than would otherwise be the case if the individual has not kept accurate records.

1) I agree there will possibly be a small time saving for individuals providing data however it will be minimal due to the relatively small amount of personal data we work with and our business model.
2) No change envisaged here again as a result of our data requirements in order to fulfill the service we provide.
3) As 2 - no change.
4) Limited benefit - each instance is a personal claim and beyond name, address, contact telephone, policy number- requires new claim circumstances data.
5) No benefit - the data trail contractually stops with us; no authority exists within any of our contracts for us to make any further use of customer personal data.
6) Unlikely.

Posted by Rhiannon R on 06 Mar 2017 5:38 PM

Hi Sallie,

Many thanks for your detailed and interesting comments.

It's interesting that you say the greatest benefactor of ported data will be the recipient. How far do you think this is linked to cost (i.e. it allows the recipient to save money)? Besides accuracy, are there any other benefits?

Do the benefits of ported data outweigh the risks, in your opinion?

Thanks,

Rhiannon

Posted by Sallie T on 07 Mar 2017 1:00 PM

Hi Rhiannon

I looked at this from the perspective of the very narrow focus of our business. I envisaged a situation of the consumer wishing to switch their insurance provider and being asked to provide a claim history. This could ultimately save time/cost for the new provider (whereas now it may involve a sales person going through a detailed script of Q & As, if the data could be transmitted automatically from one provider to another via IT systems then staffing could be reduced - having said that this would probably be initially negated by IT development costs and maintenance). It is possible that data could be extended to include the value and nature of the claim i.e. malfunction/ accidental damage/claim consistency with damage to facilitate the new insurer's decision whether to accept the risk or how to structure their quote. None of this is information the new provider couldn't currently obtain but could provide a systematised way of obtaining it.

All systems are fallible because ultimately they are driven by humans, all that can be done is mitigate the risk as far as possible and that always comes with a price tag for the business. Do I feel the benefits outweigh the risks? For my business, no I don't think I can. I do see the cost of cyber-risk insurance increasing.

Regards

Sallie

Posted by Graham B on 06 Mar 2017 5:41 PM

I am Graham, an IT Manager at a manufacturing company. We have databases of suppliers, customers and various other groups, mainly companies not individuals which need constant updating with new entries and amendments.

The main benefits of portable data to the organisation are that people are more likely to register details with new / many organisations if it is easier, the same benefits apply to them also. People will become less loyal as it will be easier to add details with new suppliers, so there will be winners and losers.

My thoughts about data protection are that companies have a legal and moral obligation to protect customer / individuals data which must take precedence. GDPR takes account of that duty but relates to the portable aspect and the changes and potential problems arising from it.

My thoughts on the benefits of portable data are:-

1) Time saving for individuals/customers makes them more likely to use different platforms without having to re register personal details, credit cards etc. benefit to organisation is more people prepared to use your services without having to enter info again.
2) Personal data supplied useful for targeting specific products or services.
3) detailed info if it includes personal preferences could be used to target likely customers, benefit includes targeting only those likely to be interested - no one likes receiving spam.
4) we could reduce cost by using existing personal data without having to request and process it, eg telesales staff having to input it from phone calls.
5) All the data can be used by anyone eg lower tier suppliers where it helps to improve services.
6) we would be at a competitive advantage by having data in this format if our rivals did not have the same access to it.

Posted by Rhiannon R on 06 Mar 2017 5:41 PM

Hi Graham,

Many thanks for your comments. It's interesting that you mentioned that people may become less loyal as they switch between different suppliers... Do you think that the advantages of this portability outweigh the disadvantages, i.e. are organisations set to gain more than they are to lose? How delicate is this balance?

Thanks,

Rhiannon

Posted by Graham B on 06 Mar 2017 6:13 PM

Hi Rhiannon,

I think suppliers will have to Up Their Game as a result of the data portability, as it will make the whole market more competitive.

I believe the advantages are mainly for the customer as they can play the market more easily. I think organisations will be the overall loser as far as this is concerned, the gains of portable data will be outweighed by having to be more customer focussed, competitive, and generally give better service than competitors.

Graham

Posted by Jennifer G on 06 Mar 2017 5:57 PM

Hi, I am Jenni and I am a Marketing Manager within the workplace training sector (for instance, health and safety and first aid training services) and work for a medium sized company which operates exclusively within the B2B sector.

With regards to data protection, I do not have overall responsibility but I am responsible for sending e-marketing communications to contact data that we hold, and I must therefore ensure the contact lists are updated regularly using our customer database and that any unsubscribes are correctly dealt with, unsubscribed from our account and not sent any further marketing communications. I must also ensure the data is not shared with any third parties and that we are transparent in the way we use data and responsive to any requests to stop using it. I would typically only be using a contact's name, company, email address and company location / address, plus perhaps details of previous courses they have booked with us.

Data protection is incredibly important, on a personal and professional level. Especially now that the use and transference of data is more fluid and more vulnerable to exploitation. When I think about data protection I almost exclusively think about it in a digital, online sense. The majority of data usage seems to be online now and relate to digital communications, although I do also think about nuisance calls that I receive, where someone has obtained my data and is using it to try to sell to me without my direct opt in. Word associations for me with data protection are a mix of professional and personal associations, including e-marketing, unsubscribes, opt-ins, data cleansing, secure online portals, password protection, cold calling, sales, marketing, third party data usage, data procurement, texts, direct mail, calls.

I am generally / vaguely aware of the GDPR, which came into force in April 2016 and is intended to strengthen data protection for individuals. It is my understanding that this initially is mainly related to personal data for consumers or service users (e.g. anything from security for people buying from online retailers to the protection of patient data) but that it will also affect businesses using business data to contact people for B2B communications. I think its a positive thing that it is looking to create more transparency and to also emphasise active consent / opt-ins for data usage rather than an 'assumed opt-in', but professionally this may make it difficult for me when managing my marketing communications as we have historically relied on purchased data from data providers to extend our reach. While this is legal, as data providers have to abide by the law, the contacts have not actively opted in to our communications specifically and so I would need to run re-engagement campaigns to ensure we have active opt-ins and look for more ways to grow our distribution lists organically.

I do not think that data portability will have any real benefits for our organisation. We typically only hold basic company details, including a contact name, telephone number, e-mail address, postal address and fax plus any specific requests for invoicing or other services or terms and conditions. For individual courses we will receive delegate names on registers so that we can issue certificates. We therefore only have their names, company name, training course they completed and the date - we are not dealing with personal data or any sensitive data. It is also not really data that people would be likely to want to transfer across other services.

We operate within the B2B market rather than B2C so I do not foresee that the right to data portability will result in any significant changes in client behaviour. As explained above, we do not hold large amounts of detailed data, just basic information to allow us to maintain training records, make bookings and maintain contact with key representatives from our client organisations. It is not data that they would have much need of transferring between organisations.

Clients may want to easily show training they and their staff have completed, and so the portability of data could help them here, where they perhaps need to demonstrate their training history to a regulatory, funding or awarding body, but otherwise I cannot imagine it having a huge benefit within the context of our organisation and sector.

In regards to the 6 potential benefits:

1) Time savings for individuals providing data to your organisation - this is a possible benefit, but as our client services team set up accounts quickly and easily on our CRM system and only need a contact name and details, plus a company name, type and size to do this, the data gathering stage is not currently onerous for ourselves or the client.
2) Greater opportunity for your organisation to acquire and use more detailed data on individuals providing data to your organisation - as a B2B company, acquiring a greater amount of personal data would not be hugely beneficial to us but it could allow us to obtain some more detailed client insights and to understand our contact base a bit more. A greater level of accuracy across data would be more beneficial than the detail.
3) Our services are agreed with businesses but can also benefit people at the individual level, so perhaps understanding more about them would help pinpoint our services more. However, I'm not sure as a workplace training company we could justify holding more detailed data about individuals. We would be better off having more detailed data about the organisation as a whole, such as number of staff, locations, any previous enforcement actions etc.
4) This is not currently a huge cost to our organisation, as explained we only need some basic info regarding contact details and basic company information to be able to create accounts for new clients and manage them accordingly, I cant see that data portability would bring cost savings for us.
5) We have previously purchased data and found it to be very inaccurate or out of date and not very fruitful. If data obtained in this way were to become more accurate, complete, consistent and reliable this could potentially have a huge benefit as we know we could target people more effectively, using accurate data so communications will land with our intended targets. However, this brings with it the issue of active opt-in, so we would still need to engage with any contacts to get them to opt in to our communications and confirm preferences.
6) At this point in time I'm not sure that the advent of data portability would create increased competition - if we were the only ones with access it might give us a competitive advantage but this wouldnt be the case.

Posted by Michael B on 06 Mar 2017 6:00 PM

Mike, Head of Product, Recruitment. We have data on candidates used for job matching that includes their email address, education, etc. I have visibility on all candidate data which includes an upload functionality for data collected offline at events and through partners. I'm responsible for ensuring the upload process performs correctly.

Thoughts about data protection: strict, compulsory. I get nervous when thinking about data protection owing to the ease with which data can be exposed when it is in electronic form. As a result, I feel data protection has become a real education piece at our organisation as it's a legal factor that has become so prominent in the internet age and should be a baseline for computer literacy in the modern workplace.

To be honest, I leave the General Data Protection Regulation to the legal people. I'll refer to them any data protection issues, but I am aware of the severe personal fines the nominated data protection employee will face if a breach is found at our organisation. When I think about GDPR, I think it's very important as protecting personal data should be a primary concern for companies dealing with big data.

Data portability will be very useful for candidates looking for jobs as they can potentially reuse data supplied to one employer for another. This would make applying for roles quicker.

I can imagine that making it easier to submit applications using duplicated data would be great for the user, however employers would get frustrated if they receive too many general applications that are not tailored to a role. This can be bad enough with CVs repeatedly used so if additional data is ported, say through an Applicant Tracking System, we might see too many repeat applications. So there's an upshot for consumers, but not for the customers.

1) Agreed for candidates (consumers) filling out forms and providing profile information such as a job history stored in LinkedIn, however there is a risk of it being used as a time saver and applications/profiles looking too generic rather than fit for purpose.
2) Absolutely, in terms of partnering with reputable sites, but we'd need to be very careful re the GDPR as there needs to be explicit authorisation from the user.
3) Potentially if a service like LinkedIn could be used to 'top' customer profiles or better target job ads.
4) As above.
5) Yes, agreed - if the data is relevant and can be accurately mapped. Might need to build consumer confidence if the service isn't directly related to where the data is coming from.
6) Potentially as our candidates could more easily build profiles on other job boards.

Posted by Rhiannon R on 07 Mar 2017 5:41 PM

Hi Michael,

Thanks for your comments.

You mentioned that the changes in data portability could increase competition in your market. What changes do you foresee this having on you as a company? Would you welcome this increased competition?

Thanks,

Rhiannon

Posted by Michael B on 09 Mar 2017 10:35 AM

Hi Rhiannon,

No problem.

The additional competition would be a challenge for us in terms of candidates being able to port their profile across numerous job boards, however whether our competition could make use of that data effectively will be the limitation on how much competition it brings. Data structures and the way candidate data is processed to match them to jobs will become more important than the base level of number of users.

Thanks,

Mike

Posted by Bob C on 06 Mar 2017 6:50 PM

My name is Bob. I am a Senior Hosting and Support Engineer. My role involves maintenance of servers and development of websites and their databases. My responsibilities in regard to data protection are to ensure that databases are kept secure and that user's data are only available to authorised individuals on the website.

I am aware of the GDPR and look forward to the update due next year. I feel that the regulations are restrictive to those bound by them but a necessity to aid in encouraging public confidence in sharing information, especially online.

Posted by Rhiannon R on 07 Mar 2017 10:56 AM

Hi Bob,

Nice to meet you!

It'd be interesting to hear your thoughts on data portability (see the questions above).

Can you see this providing any benefit to consumers? Do you agree/disagree with the listed benefits above, and why/why not?

Many thanks,

Rhiannon

Posted by Bob C on 07 Mar 2017 7:31 PM

Hi Rhiannon,

I think the right for data portability is a positive step to improve efficiency for both customers and businesses. The most obvious way I can think of would be better targeted advertising, especially when on ecommerce web platforms tailored for this, as specific types of products or services can be advertised or displayed in preference in others.

This means that any advertising or tailoring is less likely to be boring to consumers and will be cheaper for businesses, who are better able to advertise only to those consumers likely to convert.

The time saving and convenience for users is probably also a particularly significant benefit, as profiles don't need building up about a user.

Posted by James M on 06 Mar 2017 7:10 PM

I'm James and I work as an interim CTO and technical leadership consultant.

Overall I think the extent to which data portability will be a net benefit rather than a cost will be down to the extent to which a common technical method is adopted for data transfer. If a common standard does not emerge then the value of data portability is seriously reduced as organisations cannot predict the format it will arrive in, at that point there is little advantage to incoming data, a cost in terms of converting incoming data (that may be less than asking the customer to re-input of course) and a straight cost on the requirement to export data on request. Currently the GDPR only requires that data is exported in an "open standard" rather than mandating a format.

If data portability is implemented in a quick and effective form, it should increase the ability of consumers to move between suppliers of services and my clients would generally feel this is a good thing as it improves their ability to win customers via offering a better service than their competitors. This is also a benefit to consumers in that lock-in to a given service is reduced.

1) Whether any time saving is actually achieved actually a benefit relies critically on the implementation of data portability across controllers. A easy to use and commonly supported standard should achieve this benefit but I have concerns at the moment on the extent to which this will actually be achieved.
2) I think this will be a significant benefit to my clients. Reducing the requirement for customers to re-supply data is likely to improve both the quality and quantity of data held and there isn't really a situation where more data is bad for suppliers, as long as sufficient safeguards are put in place to ensure no data that may be sensitive is transferred. The question of who is liable if this does occur and this information in the used by the receiving organisation is a significant one.
3) Clearly the availability of more data allows greater opportunities. The extent to which the investment needed to utilise that information however is very dependent on the information that is supplied in practise and the costs around processing and analysing that data.
4) It's not possible to answer this question until more information on the transfer processes are available, this seems limited for SMEs at this point.
5) Very definitely this is an benefit, the re-inputing of information is a difficulty for consumers and the ability for comparison services to not only gain personal information but also information about current service use via the same channel is likely to be extremely valuable if it is realised.
6) I think it is unlikely to extend competition in the industries I currently consult with due to them tending to be B2B industries, this is not true of previous clients however.

Posted by Richard B on 06 Mar 2017 7:10 PM

My Name is Richard, I am the Compliance Manager for a SME Financial Services provider, in Investment Management and Stockbroking. I have Data Protection responsibilities for the firm.

Given the nature of our firms activities, we have to send a lot of client data to various other entities, and therefore DP is a fundamental issue we have to get right, not only for ourselves, but also with the firms receiving it. We have to ensure they meet our regulatory requirements for storage & transmitting encryption, and due diligence checks are robust.

For us, data portability is not a requirement. Our clients are already aware of the sensitive nature of their data, and that to help them and us protect it, we insist on robust protocols. Therefore when the GDPR comes in, they shouldn't really be impacted too much by way of any perceived intrusive security processes/questioning when contacting us, or, vice versa.

GDPR is very much on our radar, and are supported by our various trade bodies in helping to meet the required standards.

In reference to the 6 questions:.

1) there won't really be possibly an time saving for individuals providing data, given what we need from our regulatory requirements within financial services.

2) No change envisaged here again as a result of our current data requirements in order to deliver the service we provide.
3) No change, as same reason for Q2
4) No benefit, as again for Q2 & Q3
5) No benefit - the data is used for our services and to provide the services. the receiver of the data we send is to allow for transaction only. that provider cannot use the data for anything else other than regulatory requirements.
6) No benefit for our firm.

Posted by Guy D on 06 Mar 2017 8:13 PM

I'm Guy, and I work in User Engagement for a large IT department in the civil service. I work with our varied userbase to help them manage their data, with a variety of different business needs and demands. We store a large amount of data, but much of it we don't legally manage. We're currently transitioning it all to the cloud, which presents a variety of significant challenges.

For me, data protection is an incredibly large field. Everything is data, and even combining two sets of relatively uninteresting, or even "anonymous", data can start to produce some very useful information.

I'm aware of the GDPR much not much beyond that - we have yet to get to making any changes in consequence of it.

Data portability is unlikely to have a significant impact on our operations in terms of people wanting to take stuff out of our systems, as interactions with members of the public are generally limited to specific, one-time issues. We don't generally support ongoing relationships with members of the public. However, members of the public may well come to our users with an expectation that we will be able to do more for them, and more quickly.

For the potential benefits:

1) This could be true - though individuals generally don't provide much data that could be easily taken from other existing sources.
2) This could be true - though information provided by members of the public to us is either basic & largely public, or highly confidential. There would be potential for other organisations to more freely share data with us about our users, which would be useful.
3) This could be true - largely as above.
4) Unlikely, as information would largely be limited to public data or data we couldn't reasonably already hold.
5) Unlikely, as information would likely be largely public or highly confidential - little opportunity for commercialisation. Potentially a reuse possibility for the public sector.
6) Not applicable.

Posted by Tim M on 06 Mar 2017 8:22 PM

I'm Tim, IT Manager in Secondary Education. My data protection responsibilities are that I would be responsible for any technical (if applicable) implementations/support to meet our data protection requirements.

Data protection in it's current form stirs no particular thoughts or feelings. The upcoming GDPR does instill a little unease, not just for myself but for my organisation and the education sector.

GDPR is big on the agenda for us, in truth we feel ready however technical measures to ensure compliance are prohibitively expensive for the education sector, this meaning that it is very likely that we will have to revert to robust policy and use case scenarios. The right to deletion is one of the most interesting factors for me as there is no real technical way for us to delete information from backup files at present.

If you don't wish to read a lot, skip to the last sentence as it sums up my opinion on data portability for education.

Data portability already exists in some sense in our sector, our 'customer' data is student data and there are already ways to transfer this data between differing MIS (Management Information Systems) securely be it via the local education authority or vendor transfer tools. It is already expected that schools will give up/transfer student information when they progress from one establishment to another.

I imagine that the right to data portability will lead to a large increase in requests for data 'ports'

For the reasons above I cannot foresee any significant change for our customers or our organisation as it is already something we do.

as for the benefits:

1) I feel as though this already happens so no real change here
2) Again, this is something we already receive as we have the entire educational history of a student when they arrive.
3) Again, We already have a full picture of students educational history.
4) No cost implications.
5) We do not transfer data outside of the organisation other than to a receiving education establishment or the student after leaving upon request.
6) Competition is limited, only one of a few schools in the area is a competitor as in catchment.

In summary, data portability is a bit of non issue in my opinion for the education sector as it is something we already practice. We also already have policy and systems in place.

Posted by Olivia J on 07 Mar 2017 2:33 PM

Thanks Tim for your time and answers. As you state- your school has already been practicing Data Portability; why is this? What benefits has it offered and to who? (If any)

Many thanks,

Olivia

Posted by Tim M on 07 Mar 2017 8:33 PM

No problem, GDPR is a hot topic.

The data portability is specific to student academic and attainment data. The benefits are to either us (if we are receiving a student from another school) or to another educational establishment (if they are receiving a student from us)
It can also benefit the student/parents as they are also entitled to see a copy of this data under a standard FOI request.

Hope that clarifies.

T

Posted by Carolyn G on 06 Mar 2017 8:45 PM

Hi, my name is Carolyn. My role is in compliance, and I work in the pharmaceutical sector. Part of my role's responsibilities are to ensure that procedures relating to system and data security are adhered to. My responsibilities also include ensuring that procedures are in line with regulatory requirements for computerised systems and data security.

When I think about data protection, I think about protecting the confidentiality, integrity and availability of the data. This could be company data, personal information, medical records etc.

I am not aware of the General Data Protection Regulation (GDPR).

Overall, I believe that the right to data portability would result in tangible benefits for my organisation. In my opinion, it would be essential to be able to move data from one place to another e.g. for HR purposes, in order to maintain efficiency. This would save time.

I don't think that the right to data portability would lead to any changes in behaviour specifically thinking about my organisation. But I could imagine it resulting in changes to consumer behaviour if I think about supermarkets.

I believe that the right to obtain and reuse data would be beneficial for consumers. It is always easier to be able to transfer personal information rather than have to transcribe it.

With regards to the six potential benefits:

1) I would agree that the right would result in time saving in providing data to my organisation. For example, our organisation might be able to obtain required HR information from previous employment, rather than individuals having to supply this.
2) I agree that there is a greater opportunity for my organisation to acquire and use more detailed data on individuals but I do not necessarily think this is a good thing. I would always want to know what information is being transferred.
3) I don't think that there would be a greater opportunity to use more / more detailed data on individuals to improve services provided by my organisation as this would not be applicable. My organisation is not a services supplier.
4) There would certainly be cost savings for my organisation due to the time saved in collating data.
5) I don't think this is applicable to my organisation.
6) I don't think this is applicable to my organisation.

Posted by Emma C on 06 Mar 2017 9:47 PM

my name is Emma, I work as a CFO (finance director) for a medium size business in the retail sector, we most of what we do is around data so this is a very important area for us.

As a I am responsible for the data my business holds and uses, whether that be - employees or externally - customers and suppliers etc.

When I think of data protection, I think of the security of stored personal data we keep on people, generally nowadays stored on servers or in the cloud. Data held on people should be kept securely, only for what it was consented to be used for and should be accurate.

I feel there may be some benefit of data portability as the data collected from customers will be in cleaner and in a more format, so should improve efficiency in data collection.

Data portability will lead to changes in customer behavior, as customers will be able to use the same data with different within the same sectors, it will help them to compare and get the best deal and they will have full control over their data.

Data portability will benefit our as customers use other companies within our sector services as well alongside our product, this will be much easier for the customer as they will able to access and reuse the data held with us with other services making our product more appealing.

Potential Benefits:

1) I definitely believe data portability will be for customers, as they will not have to change their data into different formats, they will one format.
2) As the customers will have data in the same formats being used for a wide variety of companies, this would be a great opportunity to access this already completed data without having the customer having to do work.
3) This would be advantage to this more detailed data to improve our product and services.
4) As CFO I am always looking to reduce to my company so yes it is cheaper to collect detailed data all in one go.
5) I can see how there could be a greater opportunity for a sceondary market for data, such as maybe price comparison or switching but I don't think this aspect would benefit my company.
6) will increase as customers as it would not be so onerous to move their data around from one company to another.

A5.1.2 Day 2: Right to Erasure

'The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing. Under the Data Protection Act, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, e.g. where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; when the individual withdraws consent; or when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing. (ICO)'

- What are your first impressions after reading this information? Do any potential benefits come to mind (if so, what and to whom)?
- Under what circumstance do you envisage the 'right to erasure' to be exercised? How do you feel about this?
- How widespread to you expect the exercise of the 'right to erasure' to be? How do you feel about this?
- Do you envisage the 'right to erasure' to increase the willingness of individuals to provide personal data to your organisation? Why or why not? How, if at all, will this benefit your organisation?
- Do you envisage the 'right to erasure' to increase the willingness of individuals to test services that require the disclosure of personal information? Why or why not? How, if at all, will this benefit your organisation?
- Do you envisage the 'right to erasure' to lead to an increase, over time, in the accuracy of the personal data that is held by your organisation? Why or why not? How, if at all, will this benefit your organisation?

Posted by Graham B on 07 Mar 2017 10:06 AM

The right to erasure makes sense. We all sign up for things then realise it is not suitable or no longer relevant eg when considering a purchase registering with different manufacturers or suppliers, after making the purchase we no longer want emails etc relating to the subject so being able to opt out of companies using our personal data makes sense in these circumstances. From the business / supplier point of view there could be significant loss of potential trade when awareness of being able to opt out easily is understood and widely used.

I feel the right to erasure in the example above ie no longer having an interest is a benefit only to the individual, and a problem for the supplier as they are more likely to have info withdrawn.

I don't think the right to erasure will be widely understood or used. In the same way we can all opt out of spam / emails by clicking a link but many don't bother to do this or don't trust that they will be removed. That will be an advantage to those holding data.

This right could increase people to test services they might otherwise be reluctant to sign up to as they would know they can request erasure after trialling services, I personally would be more likely to do this.

Accuracy of data depends when an individual changes details. Unless there is a way of synchronising data, changes will only affect new entries after the point of change. Syncing would benefit individuals and data holders as the updates would ensure all parties have the most up to date information and neither party has to make multiple updates.

Posted by Sallie T on 07 Mar 2017 12:24 PM

My first impressions of this are from a business perspective it could be a double-edged sword: it could be beneficial in terms of volume of data held and the reduction in the amount of data secure information the company would be responsible for - my business is B2B so the data has no other use for us than as a record of the repair carried out on our client's behalf and as such our individual records are purged within pre-determined time frames that relate to our own warranties. This purge causes our systems to 'forget' and therefore the only change for us may be that requests would come earlier in the cycle but since we carry it out at the earliest opportunity in relation to

purpose of the data, theoretically nothing should change radically for us since we cannot purge during our warranty period.

In terms of business generally, I would think the downside is the massive administrative and audit trail burden 'right to be forgotten' could create and one that theoretically couldn't be accurately quantified because the business would have no idea how many customers would wish to exercise their 'right' at any given time. It clearly depends upon the nature of the business. I think it will affect those businesses who use the data for further marketing purposes, email lists etc., since it will reduce the size of their prospects pool.

In terms of my business I can see it being used infrequently, if at all. For consumers, provided the route to exercising their right is simple, I can see it being exercised more frequently to get off mailing lists or perhaps where a quote on something has been requested and the company then uses that as an invitation to continue sending marketing material. It could circumnavigate hard-selling tactics when making personal requests to stop receiving unsolicited material. Technically 'unsubscribe' should work just as well for email lists, although often it doesn't.

I think it could potentially be widespread if the media make a big song and dance about it.

Without the minimum of personal data we request via our client, we cannot fulfil our function on their behalf. Having said that, we require so little personal data willingness on the part of the individual to provide more data is not really a requirement or likely to arise. Similarly I can't currently see a situation occurring where disclosure of additional material would be necessary to test our services.

Again data accuracy is not likely to be an issue since if it is not fully accurate now, our service cannot function.

Posted by Michael B on 07 Mar 2017 1:16 PM

First impressions are the removal of the threshold is positive for consumers who do not want all their data held indefinitely by businesses or companies they purchase from. Also, this is good news for those who feel threatened by the sharing of data between companies.

I expect customers who feel they are being spammed by email or hounded by phone calls would use the right to erasure. This would be legitimate.

This seems like the sort of change in law that would not be widespread unless their was a high profile campaign against a specific business/company that was in the media for flaunting its data; or if there was strong media interest from consumer groups to point out when and how to exercise this right.

I don't think it will make much difference to the willingness of individuals to provide personal data for my organisation as any job hunt involves the sharing of personal data.

Perhaps the highlighting of upholding the ‘right to erasure’ by a service provider would lead to more individuals testing their services. Again, I don't feel this would strongly impact my organisation, but we should have a policy that highlights our commitment to the ‘right to erasure’.

We might find that the request of removal of data by our candidates would help ensure we don't have out-of-date records stored. This would be beneficial as profiling our audience would be more accurate.

Posted by Tim M on 07 Mar 2017 9:33 PM

Michael,

You make a great point about the media/consumer group interest. I can see the likes of Which jumping on this and advertising it to subscribers or even the wider public. The number of requests will definitely increase should it be reported widely.

Tim

Posted by Jennifer G on 07 Mar 2017 3:09 PM

I think the right to erasure is a positive thing for individuals / consumers and is something which was not adequately covered under the Data Protection Act. Everyone should have the right to stop their personal details being used / processed if its no longer necessary and they do not want them to be held or used by that organisation or business any more. This provides people with additional security and a route they can follow to ensure they are not hassled by companies.

I would think people would exercise the right to erasure after they had used a service but now no longer have any use for it and do not want their details to remain on record unnecessarily with a company or organisation and want to ensure they are not contacted needlessly or as part of sales campaigns that are not of interest to them. For instance, this could be when someone has utilised services for children as a parent but once their children have grown older they have no need for it and do not wish the organisation to hold their details or details of their grown up children. I think this is a fair reason to exercise this right and is a good thing for people.

I'm not sure that the right to be erasure will be widely used at first as people may not be aware of it or fully understand it. It will be used by people who are well versed in the law and perhaps in legal cases where people feel they have been persistently targeted by organisations despite requesting that the organisation deletes / unsubscribes them. I think it will be used in the same way as people using unsubscribe links for emails - some will be aware they can do this and do it every actively, others may moan about being contacted but not actively do anything about it.

The right to erasure may make individuals more comfortable with providing the necessary information to us to enable us to create an account for them and maintain contact, as they know they can have it removed at any point. This may make conversations easier and people more forthcoming and confident in confirming details such as email addresses. However, the details we process are only fairly basic anyway and are specific to businesses, not individuals, as we are a B2B business and are needed so that we can provide a service to them so they are not currently reluctant to provide these details anyway.

I'm not sure if it will encourage people to test services that require the disclosure of information more - people may still have other worries about sharing their details, such as the risk of hacking. However, in some instances people may feel more comfortable about signing up to test services, knowing they have the right to withdraw their details written in law. We dont really offer a way of people 'testing' our services though so this wouldnt have much significant benefit to our organisation. We do offer free demos for our elearning platform but do not usually struggle to get people to go for this as they only have to provide a professional email address and already know they can unsubscribe.

I feel that the right to erasure will ensure we are not wasting time / money and efforts in targeting people that are no longer interested in our services or for who they are not relevant for, but it will not make our data more accurate overall. I also cant see our clients using it much so I do not think it will significantly change the data we hold.

Posted by James M on 07 Mar 2017 4:35 PM

It certainly has an at least theoretical benefit to the consumer in terms of managing the extent of their personal data, but I agree with other commenters that it is unlikely to be exercised much in practise except in media promoted cases.

I think it is highly unlikely that the right to erasure will change consumers behaviour with regards to providing information either for long term usage of services or for trials, in general customers provide information as a necessary or at least expected requirement to receive a given service and I do not believe that significant consideration is given to the likely length of retention at the point of supply.

For most of my clients, requirements around maintenance of records (e.g. PCI) would mean that the right to erasure would only be exercisable by a customer 5 years of more after the data was collected, so I do not see it likely to be a significant burden in the short term, however being able to reliably determine the location of data in data management areas such as warehousing and third-party services such as bulk mailers is likely to have a significant burden at the point at which the data is needed to be found. A lot of data storage is currently more ad-hoc than is ideal for audit purposes.

There is an also an issue with data being passed between companies, I'm not currently clear whether when a 'right to be forgotten' request is received by a company then that company is required to then forward that request on to any third parties who may have received the customers information, and whether that request would then need to be forwarded on to the next level and so on, as well as to the extent to which customers have an ability to be informed as to which companies hold personal data on them and the content of that data.

Posted by Carolyn G on 07 Mar 2017 6:34 PM

I am happy that the GDPR will provide the right to enable individuals to request deletion or removal of personal data whether or not there is a compelling reason to do so. In my opinion, what happens with personal data should be at the discretion of the individual and if they want it to be removed then it should be. Costs associated with this should be offset by efficient procedures and processes. I believe that individuals will benefit from this as they will feel they have more control over who stores their data.

I can think of numerous examples of where the right could be exercised. If some personal data is stolen, then individuals may then want their data to be removed in case their data is at risk. If an individual finds they are receiving junk mail, they may request that a company deletes their personal data. These are just two examples. I feel that the right of individuals to request this and for it to be carried out is important.

I believe that in the future, right to erasure will be exercised more and more. In some ways, I think this is a good thing as people are registering their personal details with more and more companies, websites etc., and people do tend to forget who has their details. Perhaps individuals will keep more records in the future, and request deletion / removal more frequently.

I don't envisage the right to erasure to increase willingness of individuals to provide personal data to my organisation as I can't see how this would be applicable, other than for human resources.

I believe that if individuals understand their right to erasure then it perhaps would increase the willingness of individuals to test services that require the disclosure of personal information. I think this because the individuals will know that their data can be deleted or removed. This will not benefit my organisation in any way that I can see, as it is probably not applicable.

I don't think that the right to erasure will lead to an increase over time in data accuracy held by my organisation. The only personal data I can think of that is stored is that by human resources, and I can't see how the accuracy of the data would increase due to the right to delete data.

Posted by Paul M on 07 Mar 2017 7:17 PM

In response to the 6 points above:

1) For me the obvious benefit is to build up data that is closer to a census. This will make target marketing more accurate, which will help enhance consumer sovereignty.
2) If a consumer has had a bad experience with a company it seems fair that erasure is allowed. Personally, I am not sure whether the GDPR threshold is necessary. How many people exercise their rights?
3) I imagine that the 'right to erasure' will have little impact on most people. The benefits seem more obvious from the seller's point of view.
4) Yes, but only marginally. Most people who are happy/ unhappy to give information about themselves will continue in the same vein.
5) As above- it may help things slightly.
6) Yes- it will, or at least it should. Much will depend on how well each organisation deals with its data. I have lived in my present home for 13 years. We still receive post for the previous owners. So it is my belief that there are good and bad companies and all points in-between. Some organisations are good with all things data-related, others not so.

Posted by Bob C on 07 Mar 2017 7:49 PM

My first impression is that this is a pain to implement, especially in cases where businesses need to erase e-commerce data but also need to anonymise CRM records, which may in turn be used for accounting. I feel this is a necessary regulation to provide further confidence to Internet users.

I would expect the regulation to be mostly applied to information that is collected and in the public domain, such as published reviews or social media activity. I feel that it is particularly important to be able to erase published information like this especially for abuse victims in need of protection from being tracked down. This regulation is also important because everything we do online is recorded, data offered often without thinking and can be used for identity theft. As users' views change, so too could their decision to have information about them recorded.

I suspect that the right to erasure will encourage the provision of information for market research or signing up to goods and services online, as they will hopefully aware that information shared can have a definite lifetime that can be determined by them. I believe that this will have the knock on effect of more accurate data being offered, as it can be withdrawn if a user has second thoughts about what they share.

I don't imagine that the right to erasure will be exercised often for the websites I support, as the most sensitive data relates to e-commerce baskets and addresses, which are unlikely to be abused by reputable businesses.

Posted by Tim M on 07 Mar 2017 9:25 PM

Bob,

I agree that people are probably most likely to 'request erasure' from sites they think will harm them. Especially if for instance, students have left university and are cleaning their digital footprints to apply for jobs and get rid of their embarrassing night out photographs in bulk.

To that end I think that the likes of Facebook, Twitter, Instagram etc... are going to receive a lot of requests. Whether they will have to comply or not is another thing entirely, If they archive the data outside the EU does that cover them? Are organisations likely to start keeping encrypted off site backups in countries outside the EU to avoid GDPR? Of course I haven't explored the legal complexities of this, it is just something that springs to mind.

Tim

Posted by Emma C on 07 Mar 2017 8:34 PM

First impressions are that right to erasure will be advantageous to consumers, as it will give them much more control over how their data is being used, and if they decide they no longer want to use a service, a consumer will now be able to request deletions details, I certainly think this change is a good thing.

I expect the right to erasure will be used more so, when a customer is not happy about something, for example receiving spam emails and advertising after providing their data to use a service. In these instances, I feel it is justifiable for a customer to request personal data to be deleted as they are withdrawing their consent.

Not sure how widespread right to erasure will be, I think it will be mostly be used by customers unhappy about the way their data is being used, or perhaps by people whose circumstances have changed so the data is no longer accurate. Also by those who are withdrawing consent for other reasons, such as, maybe they consented when they were young and no longer consent in adulthood. Also, I presume in certain circumstances employees could request data be erased but I presume this also would not happen often.

I imagine customers will feel more secure knowing that their data could be erased when they request it under GDPR, knowing that the data can only be used for what they have consented it to be used for.

Customers may be more willing to test services, knowing that they can erase personal data at a future point if need. we sell test products, and so this may have a small positive impact on my as customers if they had been unwilling to sign up previously due to having to provide personal data.

Keep data records up to date and accurate is key to my organisation, some of the products we sell are subscription based, my only worry is that one of our key performance indicators is customer retention rates, this may be a bit harder to calculate if many customers are requesting that their data be erased.

Posted by Tim M on 07 Mar 2017 9:29 PM

Emma,

I agree that disgruntled people are probably most likely to exercise the right and also with the young vs. old argument. We spend an awful lot of time trying to educate about a students 'Digital Footprint' and the effect it can have post education.

Tim

Posted by Tim M on 07 Mar 2017 9:14 PM

I am going to write this before reading others to ensure it's my thinking!

The right to erasure is something I touched on in my introduction yesterday. I will elaborate our thinking on this subject at the end and welcome feedback from the forum.

My first impressions are that it seems like a sensible idea and the idea that you do not need a specific reason to request removal is a good one. I guess it is a natural extension to the 'unsubscribe' link on circulars but for all your data. The benefits I can see for an individual are great for one hypothetical instance; *I once had a Facebook account, I no longer want that Facebook account and I don't want the ability to re-activate my account with all my data at a later date so please delete my data.* I cannot see any particular benefits to my organisation, I can see a potential for a large number of requests when the GDPR is effective and it is in current news. I guess as time goes on things will calm down a bit.

I think the right to erasure in a general will be used by many people, myself included to request removal from as many databases as they can as soon as they can. I feel this is generally a good thing.

As above I imagine that companies would be inundated by requests whilst it is still a topic in the news etc... but i expect after a while the number of requests will gradually decline. In the short term it worries me as staffing levels have reduced and budgets been cut. I think a very real approach education will take is to outsource the record keeping to external data storage and indexing companies.

Our customers don't really have a choice as to what data they share with us. Their data is like a passport, there are elements which have to be present so i don't think this make any difference to us as an organisation.

I'm not sure we would see an increase in people testing us, but I imagine larger corporations may see this, especially those in sectors where circular emails tend to originate.

Our organisation is already partaking in a programme of ensuring our alumni data is correct and ex students and staff have ticked the box to allow us to keep their data. The downside to this is that our software allows us to 'Archive' people but it also allows us to 'Unarchive' people. There is currently no option in the GUI to delete a person, this I imagine will be patched fairly quickly as it has been reported. Streamlining and ensuring our data is 100% correct, GDPR or no GDPR is a great thing, but the acronym helps to speed things up.

To follow up on yesterdays concern. I would be interested to hear peoples views on the contents of backups. Does anybody feel that the 'right to erasure' would extend to backups. I cannot see any particular exemption or guidance for backups, but I also see no way to delete the data held in the

backups without creating a prohibitive workload or destroying the entire backup set which of course is not an option. At this stage, I see the right to erasure as the biggest alarm bell for organisations and an example of where I think bullet proof policies are likely required as at present there is no technical solution that we can see.

Additionally, Since the Goddard inquiry (Independent Inquiry into Child Sexual Abuse) schools have been advised to keep all data (MIS, emails and files, student and staff) indefinitely so that it may be available to the inquiry. Not only does this seem to contradict the whole 'write to erasure' premise, it also leads to a headache for data storage.

Posted by Guy D on 07 Mar 2017 10:22 PM

1) Our users are unlikely to have a purpose for using data once the original request from the member of the public has been dealt with, though they may wish to stay in touch with them.
2) This wouldn't create an additional burden, as our users will sometimes receive requests for the data they hold to cease being used and to be deleted, within the current scope of the DPA.
3) No more widespread than at present, though potentially greater if it becomes more known about as a "right".
4) Unlikely to have any impact, as their public's reason for contacting our users will still be the same. It may provide them with more confidence in how the data will be handled.
5) I don't think this is applicable to us.
6) Unlikely, as personal data is either refreshed from public sources on a regular basis, deleted or archived and not referred to. Users are unlikely to exercise this right actively.

A5.1.3 Day 3: Subject Access Requests

'Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed; access to their personal data; and other supplementary information. You must provide a copy of the information free of charge. The removal of the £10 subject access fee is a significant change from the existing rules under the Data Protection Act. (ICO)'

- What are your first impressions after reading this information? Do any potential benefits come to mind (if so what and to whom)?
- Under what circumstance do you envisage the 'right of data subjects to access their data' to be exercised? How do you feel about this?
- How widespread do you expect the exercise of the 'right of data subjects to access their data' to be? How do you feel about this?
- Do you envisage the 'right of data subjects to access their data', to increase the willingness of individuals to provide personal data to your organisation? Why or why not? How, if at all, will this benefit your organisation?

- Do you envisage the 'right of data subjects to access their data', to lead to an increase, over time, in the accuracy of the personal data that is held by your organisation? Why or why not? How, if at all, will this benefit your organisation?
- Do you envisage the 'right of data subjects to access their data' to lead to changes in your organisations data sharing practices? Why or why not? How, if at all, will this benefit your organisation?

Posted by Graham B on 08 Mar 2017 10:31 AM

Main benefit is to individuals due to the removal of the access fee. This could be a burden to data holders when people get used to the idea that they can request data free of charge and take up this option en masse.

Individuals are likely to request data if they feel they are receiving excessive or inappropriate mailshots to see what data is being held about them. This is an incentive for keeping data upto date and targeting mailshots accurately to avoid putting people off and regarding mailshots as spam.

I think individuals will not be generally aware of their rights and perhaps will not be bothered to exercise them which would be a benefit to companies as manpower or automated systems would be required to handle the requests for data which is unlikely to result in sales.

This ability to access personal data held about yourself is more likely to encourage people to give their data as they know they can keep a check on it and request deletion if incorrect or excessive data is held. This would benefit the companies holding info as its more likely to be full and upto date leading to an increase in accuracy. This benefits all data holders as the target email / address / requirements of individuals will mean targeting effectively.

Sharing data would enable upto date info to be shared giving an advantage to all companies sharing data, the only potential problem is where two sets of differing data are held for an individual, it would be difficult to know which was the most recent / correct unless some form of date tagging of changes was in use. If upto date data is shared targeting would be more effective, eg not sending to obsolete email addresses.

Posted by Sallie T on 08 Mar 2017 4:59 PM

I can see no benefit to business in general and in fact an administrative headache with attendant costs. The individual will of course benefit from the removal the current fee.

For my own business, I can say that in 14 years we have never had a request, as for the future I can't see that changing due to the nature of what we do and the small amount of data we process. I think exercise of this right all depends upon the nature of the business and the type/level of detail of information held.

It is possible that the removal of the fee may generate an increase in exercise of this right fuelled by curiosity however I think if an individual has a very pressing need or desire for this information they would exercise it anyway irrespective of the current fee.

I foresee no change in the willingness of individuals to provide information to our business, nor would any more information be of any benefit to us since we have no need for it.

Due to the nature of our business, once the warranty has expired on the repair work we carry out, we have no need to retain any information about the individual. We verify the individual's information at the outset of the relationship and aside from contact details changing (which we wouldn't expect or require to be notified of although would anticipate that the individual would notify their insurer of changes/inaccuracies) nothing would alter during the 12 months post repair. If there is a warranty claim during that period, we re-verify the contact information with the insurer the time of the claim. So right of access has no real impact on us from the perspective of improving accuracy.

No change for us on data sharing, we are the end user of data provided by insurers.

Posted by Michael B on 08 Mar 2017 5:30 PM

This seems fair to the consumer - the £10 fee would be enough to put all but the most ardent off requesting access to their data. Businesses will be less impressed as they could be inundated by requests for data, however the benefits for the consumer feeling more in control of their data and how it's used is very important.

I suspect it will be used where a consumer is worried about the type of data stored on them, and might be sparked by an unfavourable news story about a company about data usage, such as Google or Facebook's use of personal data for advertising. This is a good thing from a consumer perspective, but will be time-consuming and potentially damaging for advertising platforms that use personal data for targeting.

I doubt the 'right of data subjects to access their data', to increase the willingness of individuals to provide personal data to your organisation, unless there is media attention about the serious mis-use of data following someone using that right to obtain evidence. For my organisation - recruitment - users may be keen to check they have an up-to-date CV or personal information on their file before submitting applications, which is a good thing as it would improve application quality.

Whether the 'right of data subjects to access their data' will lead to an increase, over time, in the accuracy of the personal data that is held by my organisation is unlikely as our users will tend to update their profiles and CVs regularly.

The 'right of data subjects to access their data' is unlikely to lead to changes in my organisation's data sharing practices as we will always be expected to share personal profile data with employers as part of the application process on our site.

Posted by Jennifer G on 08 Mar 2017 5:45 PM

My first impression is that this is a positive change for consumers / individuals as they can check what data is being held about them and ensure its accurate, complete, relevant and appropriate for usage without having to incur a fee. It gives them the basic right to know what information people have about them. For companies that hold such data it could be a negative thing as the same amount of manpower will be involved in providing the data but they wont receive a fee for it, and requests could increase now that individuals are not having to pay for the privilege.

People might access this data if they suspect that people hold incorrect / inaccurate information about them and that, as such, they are being sent communications that are irrelevant or are perhaps missing out on communications, or even benefits, that are appropriate for them. They may also want to know what data an organisation holds about them before closing an account or making other purchase decisions with other companies. I think its a good thing that people can check data

and ensure that the communications, benefits or services they are receiving are suitable and well tailored for them - this ensures better use of everyone's time, both the individual and the organisation that holds the data. It ensures people can be more targeted in the way they use the data.

I don't really expect the exercise of the 'right of data subjects to access their data' to be that widespread, as many people will not be aware of the right, unless a big awareness campaign is launched and may not understand it or how it could or should be used. For people who are data savvy, however, and who do understand the right, it might make them more inclined to access the data now they know that no fee will be charged. So it may mean a small increase for those who would have wanted to previously but were put off by the fee. I feel comfortable with this, I dont think it will be widely used enough to have a detrimental effect on organisations, and I dont really think it would have an impact on our business. I cannot see this being exercised by our B2B customers.

The fact that individuals can access their data, together with other rights to be able to have it erased etc, will work together to make individuals a little more willing to provide personal data to our organisation. They will feel more confident that they will be able to access, check it and change it at any stage. However, as we don't hold much personal data and deal with B2B, holding only basic company information and professional contact details for individuals, I dont think people generally feel reluctant to provide us with data now and so it won't have a huge impact or benefit to us.

The fact that individuals can access their data easily should eventually result in data in general being more accurate. I think this will take time, as I dont expect a huge uptake initially. For our organisation specifically, I'm not sure it will lead to data being more accurate as we mainly only hold basic business information and basic personal details for the purposes of certification and assessments. As people are undergoing training for which they need to be certificated and need to evidence they completed it, they are generally happy to provide accurate information and it is only basic information which does not need to be held for more than 3 years (courses generally refresh within this timeframe).

We don't really share data with other organisations, except for when required by accrediting / awarding bodies to check assessments and course attendances, etc. The ‘right of data subjects to access their data’ would not affect our practices.

Posted by Bob C on 08 Mar 2017 7:12 PM

My first impression is one of concern. Even where a piece of software has the ability to provide all this information at the click of a button, this request would cost half an hour at least, once communication time has been accounted for. Bearing in mind other regulation around secure sharing of personal data, there are other potential issues in authenticating the request, which also costs time. This could become very expensive to fulfil, especially when there is no cost to the user requesting the data to discourage users from making requests simply because they can.

I can see that there would be a benefit to users because they would hopefully be more comfortable sharing data when they know they can freely access it to check what has been shared and how much.

I would expect this right to be exercised a little more than it currently is, as some users may be curious to see what data is held about them when the request costs nothing. I also would expect to see some requests from some users who want to be a nuisance or financially harm a company who

has given them a poor experience. We will only know more about this once we see the regulation implemented.

I believe the right of data subjects to access their data is likely to increase the accuracy of data, as it can always be reviewed and corrected and there will hopefully be a knowlege that data provided can be reviewed and removed (as discussed yesterday) if the data found in the review is undesirable in hind sight.

I suspect that my company will review the change in number of data requests and if sufficiently high then implement a solution to automate the data extract as much as possible. This is unlikely to have a negative effect on my organisation, as the client will most likely be tired of paying to have data extracted manually and would rather buy an automated process.

Posted by Paul M on 08 Mar 2017 7:39 PM

In response to these questions:

- In reality I am not sure that it will make that much difference to things. Those who want privacy will be largely unaffected. The £10 removal is welcome, although it will not lead to a rush of activity.
- This is absolutely fine. In the way that some people insist on receiving no direct mail, then there will be people who exercise this right. There are simply those people who do not want to be part of any marketing activity if they can help it.
- I cannot see things changing much at all. Most people are happy (tacitly or stated) to have their information used for marketing purposes.
- Perhaps, although if so only marginally. It is not a high interest or concern to most consumers- most people are really not that bothered. My firm will probably not benefit greatly- most of our clients are professional audiences, not consumers.
- Yes, slightly, although its implementation is currently of limited use to us. I am not sure that the information given by consumers will be more accurate but over time holders of data will hopefully iron out any inconsistencies.
- No. GDPR is of limited relevance to my company. However, as we move into more consumer spaces it may help us, although I am not convinced that accuracy levels will be much better than currently.

Posted by Tim M on 08 Mar 2017 7:53 PM

As with previous questions, it is clear that this will benefit consumers tremendously, not having to pay anything to request such information will help those not wanting to pay and i think it is probably fair to say that your data is your right. I do not see any organisational benefits.

I think some people may use their right of data subject access as a random request from multiple organisations. This could increase workload but I imagine most will use the right if they have an issue with a service and want to see what data is held.

I don't feel this will be particularly widespread unless heavily publicised, again i imagine these types of requests to reduce over time. I don't feel that there will be any significant increase in my sector.

As discussed previously there is little choice what data is provided to us for individuals as it is more like a passport or record. I don't expect this to be much of an issue for us. No benefits, no drawbacks.

Accuracy of our data is key, incorrect data can have a huge effect on students so the current data is already reasonably accurate (bar the odd data entry error) Alumni data is an area of concern, I feel we need to come up with an opt in system for us to retain alumni data.

I don't think that the right of data subjects to access their data to impact the organisations data sharing practices at all so again, no benefits, no drawbacks.

Posted by James M on 08 Mar 2017 8:33 PM

A concern I have regarding the scrapping of the fee is an increase in general requests over time, or in bulk at a specific time due to either social or traditional media attention (I believe this was the original reason for the charge rather than any assessment of the actual cost of generating the response). Particularly the latter could results in large and unexpected costs for those businesses that are unable to respond to requests in an efficient manner.

I think it is unlikely that right of access will make a material difference in the willingness of customers to share data. The information collected by my clients is generally information customers are used to sharing with organisations such as name, address etc.

An increase in accuracy I think would only be achieved if, in responding to the necessity to provide access to personal data, a mechanism is put in place whereby that data can be accessed trivially, e.g. via a "My account" page or similar. If a request needs to be made which cannot be fulfilled instantly I do not believe most customers will utilise the ability purely as a data verification technique in most cases.

With regards to data sharing I think there are two sides to consider, one is data sharing back to the customer and in this case I think it will encourage more proactive data sharing with customers to reduce costs of responding to requests, with regards to sharing data with third parties I think this will probably result in a reduction or at least more concern around this given the question of needing to confirm to customers how and where their data has been shared.

Posted by Emma C on 08 Mar 2017 9:33 PM

Of course individuals should have be able to access their personal data free of charge, I am happy the £10 charge is being abolished so this will be of benefit to customers. From a business point of view, I worry about the cost of increased administrative burden of many requests, which the £10 charge would have covered now businesses will have to take the hit.

The ‘right of data subjects to access their data’ would be exercised in any situation a customer wants to check what data a company has on them, maybe to check accuracy. I often wonder what data companies have on me, on so I would personally be interested in using this option.

How widespread this would be I am unsure, I guess it would be dependent on how much publicity and media these new regulations get, and I expect there would be a surge of request at the beginning and then the requests will level off to a low level. The fact the £10 charge will be abolished could be a further incentive to people to now request it, as imagine having to request this info from a couple of companies under the current Act these charges could soon rack up.

I am not sure if this will help my business though it definitely will not hinder it, I guess it is just an added benefit to the customer and they can put their mind at ease that they can access their data if needed. We do not share a lot of data with other companies, so individuals being able to access their data would not have any effect on this.

Posted by Carolyn G on 09 Mar 2017 4:46 AM

I am happy that the £10 subject access fee is no longer going to be imposed. I don't necessarily see any benefits other than for the individual being able to obtain their information or records free of charge.

Access to medical records comes to mind as one example where people might exercise their right. I believe this is only fair. In addition to this, other examples might include an individual wanting to access college and university records where these have previously been lost. Again, I feel it is a good idea.

I don't believe that exercising the right will be very widespread. Individuals generally have a specific reason for wanting to access the data that an organisation holds. I don't see it being something that will happen all of the time. I do think that if it were to happen very regularly then it could put strain on organisations to meet requests due to time to process.

I don't think that the right will impact my organisation at all. Individuals do not provide personal data to my organisation other than for HR purposes. I also therefore don't believe that the right will lead to an increase in the accuracy of personal data that is held by my organisation or any changes in my organisation's data sharing practices (not applicable).

Posted by Guy D on 09 Mar 2017 12:38 PM

1) Few potential benefits really - data held by our users on members of the public will almost always have all been provided by them themselves, or from public sources, so they will know about it already.
2) I can't envisage many, if any, situations where this would be exercised.
3) As above - very unlikely.
4) Unlikely - individuals are generally have a direct interest in their data being processed, and this wouldn't add much.
5) It could do, but unlikely for the same reasons as in the previous day's question.
6) Unlikely, as it will remain pretty uncommon.

A5.1.4 Day 4: Data Protection Officers (Section 5, Art. 37- 39)

'The role of Data Protection Officers (DPOs) is to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws; to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc). (ICO)'

- Does your organisation have a DPO? Does it need one?
- What are your first impressions after reading this information? What impact if any will this have on your organisation? (Positive or negative.)

- Do you envisage the DPO to interact directly with individuals whose personal data is held by your organisation? Why or why not?
- Do you envisage that the role of DPO will have any positive impact on your organisation's reputation? Why or why not? What would the benefits be?
- **Below is a list of potential benefits of having a DPO**- please explain if you agree or disagree with each potential benefit and why you think this:

1) Increased status/priority of data protection within your organisation
2) Reducing the cost for individuals to exercise their data-related rights (e.g. in terms of accessing their data)
3) Having a positive impact on data security in your organisation (e.g. lead to a reduction in the risk of data breaches)
4) Having a positive impact on the quality and accuracy of data processed in your organisation

Posted by Michael B on 09 Mar 2017 10:47 AM

We don't have a DPO that I'm aware of in our office, but we do have someone in finance who acts as a data controller of sorts plus legal consul who is an expert, however I do not know if they would be classed as a DPO. I believe a visible DPO would be hugely beneficial given all the topics we've covered over the last few days.

A DPO sounds like a positive position in terms of safeguarding our data practices.

I'd like the DPO to be there for reference by those who have contact with candidates, but not be expected to speak to them directly as it does not strike me as a customer-facing role. I'd want them to be focused on how data is collected, storedm and securely shared or deleted as appropriate rather than answering calls and emails. They should get feedback from users, however, as it would inform their role.

Having a DPO should be positive as it shows a dedication to proper data storage practices.

1) Agree - they would be the gatekeepers to how data is handled.
2) Potentially - I'd want the DPO to put a standard practice in place for dealing with the data rights of individuals but not be responsible for day-to-day activities. Perhaps an assistant or other team could ensure the procedures are followed.
3) Agree - the DPO should totally be leading on data security.
4) Agree - they should be able to ensure data is collected responsibly and entered into the database effectively.

Posted by Bob C on 09 Mar 2017 10:55 AM

My organisation does have a DPO that the DPO is necessary. The role of DPO is not often called upon day-to-day so is taken on by one of the directors among other duties. Since there's not a lot to be done day-to-day, there aren't any negatives. I think it's great that we have a DPO to oversee planning and implementation of new systems for data storage. I would expect the DPO to interact directly with individuals to provide maximum oversight.

I don't think having a DPO has an impact on reputation because I don't think it's something my company really shouts about. Perhaps we should in order to improve client confidence.

I think that having a DPO does increase the status and priority of data protection within my organisation, certainly internally, as having a DPO encourages a culture of awareness and consideration when handling data or setting up systems for recording it. The DPO therefore has a positive impact on data security, quality and accuracy, as these are all considered during the planning and impementation of solutions for the client.

I don't think having a DPO reduces the cost for individuals to exercise their data-related rights. If we had no DPO, there would be another client facing member of staff who would relay the request to a developer to extract the data anyway.

Posted by Paul M on 09 Mar 2017 11:23 AM

In answer to the four bullet points:

- No. We are only a small company, and most of our work is b2b. I keep my colleagues up-to-date with data protection issues.
- It will have little impact. I am on top of things and this new information is something we'll take in our stride.
- Possibly. It would be my responsibility to interact with anyone with a data protection query.
- Not really- I don't think we need one yet. Also, we are small enough to control things and take responsibility.

In terms of the benefits:

1) We are very respectful of data protection. We don't really need an increased status for it.
2) This is not really relevant to us, but I can see that it may well help larger companies and those dealing more with consumers.
3) As far as I know we have never had a data breach, so I am not sure about this.
4) Again, I am not sure how relevant this is, although I can see that this may well help larger, more consumer-focused, companies.

Posted by Sallie T on 09 Mar 2017 11:50 AM

1) Part of my role involves full scope of DPO responsibilities although I am not the person registered as Data Controller with ICO. Yes we definitely need one to ensure compliance, adequate training,management etc., and fulfil our contractual obligations regarding training and compliance.
2) I don't generally not interact with individuals external to the business whose data is held regarding their data but if the need arose, such as say a breech situation, then obviously I would have to. I do interact daily with all employees whose data (HR records etc.) is held although again this does not necessarily relate to the data we hold (outside of induction processes when it is explained to them what is held and what their rights are). From a training and compliance perspective with our corporate responsibilities and data security per se, then I interact frequently.
3) The positive impact is felt in a number of ways, primarily the company's ability to process data within legal parameters by ensuring our staff are fully trained, systems and procedures fit for purpose and the company compliant. This equally ensures our clients' confidence that we are capable of handling their customers' information without detriment to the customer or reputational damage to the client.

4)

1) Given the nature of our business, despite the fact that we directly collect very little data, because the devices we repair can contain vast amounts of personal data, data security has paramount importance in our business already. Increased status and priority helps my business case when advising board members (whom may not necessarily fully understand the implications) on needs and requirements to fulfil our responsibilities in this respect so it is to be welcomed.
2) I'm not sure I see the role of DPO assisting in cost reduction for individuals since we currently have a very simple and clearly defined route.
3) Yes, see 4.1.
4) Yes. Our systems have had to be designed to validate the accuracy of data at the outset in order for the system to work. Any development work is done in conjunction with stakeholders and thus includes myself in respect to data compliance, protection and security.

Posted by Guy D on 09 Mar 2017 12:45 PM

Our users are their own data controllers, but in practice they will delegate all responsibility for this to their own staff. Having a member of their staff identified as a DPO would be beneficial for them, and for individuals, as they would (hopefully) be more aware of the responsibilities associated with data protection generally, and take more personal responsibility for ensuring that proper procedures are followed. They would interact directly with individuals, as this is already a large part of their work, and this may have a positive benefit for the reputation of our users, though this is likely to be limited.

1) Agree - anything that can increase the importance and status of data protection for our users would be good.
2) Marginal - this isn't something that would happen often, so not likely to see a huge change here.
3) Agree - by specifically allocating a particular person to do this, hopefully more care will be taken with data processing.
4) Agree, though not to a huge extent. This is generally the responsibility of all staff.

Posted by Jennifer G on 09 Mar 2017 5:09 PM

We do not have someone who is named specifically as a DPO, as far as I am aware, however our Corporate Services Director has responsibility for overseeing data protection and manages things such as our Data Protection registration currently. She would act in this capacity. We probably do not have an urgent need for a DPO but someone who has responsibility for this area would be useful and beneficial to us.

I think its a positive thing to have a named person with specific responsibility to ensure there is clear accountability and ownership for data protection issues and someone who can help to guide others and ensure the company remains compliant with the GDPR and other data protection laws. I think this will be positive for my organisation, as I said we already have someone who oversees data protection but without the formal title, and the added provision of staff training will help to ensure everyone is more aware of data issues.

I would think that the DPO would not interact directly with individuals whose personal data was held by our organisation in the first instance. This would mainly be account managers. I would expect

the DPO to only interact directly if an individual made a request relating to the GDPR or an issue was escalated. This is because the DPO would not be dealing day to day with processing information but would take on the role of overseer, auditing the processes carried out by others. They also would not directly deal with clients but would then get involved if any data issues arose.

Having a named DPO probably wouldn't have a major impact on our reputation in general but would be beneficial for the tender process when we are bidding for new contracts - it would show potential clients that we have all data protection requirements in hand and a robust process for ensuring we remain compliant. To our general client base, it would probably be nice to know but not a major priority for them initially. We are an IIP Gold employer, a Living Wage Employer and an approved centre for many regulatory and awarding bodies - in our sector that is much more important to our client's in the first instance. If the profile of the GDPR was high and awareness grew though, it may help that we could say we had a DPO in our organisation.

In terms of the benefits:

1) I think having a named person responsible with clearly defined roles and responsibilities will ensure data protection cannot be ignored and will become a higher priority, so I agree that this will ensure we have it more firmly on our agenda and can ensure we're complying with the law.
2) There isn't a major cost involved for us right now if this were to happen, and the processes wouldn't change majorly with an identified DPO in place so I dont think we would experience this as a benefit.
3) I agree because, as with no 1 above, it will mean someone is taking ownership of data security and it will make us more accountable and transparent and increase awareness and education across the staff team, thereby decreasing the risk of data breaches.
4) We do not tend to have an issue with the accuracy of current client data as most of our clients are happy to provide data and we only hold basic company and course attendee information, so currently I do not foresee that appointing a DPO will make much difference to the quality and accuracy of our data.

Posted by Graham B on 09 Mar 2017 6:28 PM

I am effectively the company DPO, but unofficially as we need someone to carry out these duies.

First impressions are that its good to formalise the position as it gives better authority to carry out the duties.

The DPO would interact with other staff members but it is for lower level staff to interact directly with individuals whose data is held, otherwise the DPO could never manage their workload.

Having a formal DPO enhances the companies reputation as it shows they take data protection more seriously.

Potential benefits

1) Agree because it shows the company takes data protection seriously.
2) I don’t think a DPO will be able to directly reduce costs apart from small measures to make departments more efficient.
3) Agree as someone will oversee and ensure pro active measures to prevent data breaches.

4) Agree as they will co ordinate all departments and staff and implement plans to streamline systems and working practices.

Posted by Carolyn G on 09 Mar 2017 8:21 PM

I am unsure whether my organisation would need a DPO specifically for the purpose of ensuring compliance with the GDPR. However, our organisation does have staff who have responsibilities for ensuring compliance with other data security requirements. The data security requirements (aside from the personal data requirements) applicable to my organisation are to ensure security (confidentiality, integrity and availability) of data generated to provide evidence that the company complies with other requirements.

Having specific personnel in place to ensure that the GDPR and other data protection laws are being complied with along with other responsibilities seems like a good idea. Therefore, I think this is a positive thing. As stated previously, I'm unsure of the requirements to have a DPO specifically for our organisation - although I could see this would be needed for HR purposes.

I don't envisage the DPO to interact directly with individuals whose personal data is held by my organisation. The only data that would fall under the personal data requirement would be HR data.

I don't think the role of DPO would have an impact on my organisation's reputation as it would be limited to HR data.

With regards to the potential benefits listed:

1) Disagree for my organisation as this would be limited to HR data. Data protection would already be a high priority.
2) DPO role could potentially result in a reduction in cost to an organisation as there would be a specific person in place to ensure that processes are efficient.
3) I believe a DPO would have a positive impact on personal data security within my organisation but again this would be limited to HR data. A DPO would ensure that personnel understood the requirements and this would lead to greater data protection.
4) I don't believe this would be impacted. Personnel can check accuracy of their HR data themselves.

Posted by Emma C on 09 Mar 2017 9:01 PM

We have an Information Systems manager who registered with the ICO, the overall responsibility comes under myself and other directors. Yes the role of the DPO is relevant within my however at the moment data protection responsibilities take up a minimal amount of time. So my first impressions of reading the above is actually that is a lot of responsibility, and with the GDPR I think more training would be required to make sure they are up to speed on legislation. my view is a positive one as it is great to have an an expert to deal with all GDPR responsibilities, the negative would it will be more time consuming for the individuals taking their time away from their main responsibilities within the business.

No, I assume requests would be processed by customer service and customer service would seek out the DPO for any additional advice on how to process these request I doubt they will directly interact with these individuals.

I think it will have a minimal positive impact I doubt having a DPO will really be a selling point, it may put some people's mind at ease to know that their data is being processed by an organisation with a DPO but this would appeal to very few people I expect.

In answer to the potential benefits:

1) Having a DPO would increase the status of data protection as the having a figurehead, an expert for people within the business to turn to, it shows the business is taking data protection seriously.
2) I cannot see how having a DPO would reduce costs for people accessing their data so no advantage there.
3) A DPO would help prevent data breaches as they will be training and advising staff on how to keep data secure and what their responsibilities are regarding data protection. They are also ensuring system are robust and compliant
4) Accuracy of data would improve again because the DPO will train others on the correct way to process data to comply with GDPR, collected data should therefore be more accurate.

Posted by James M on 10 Mar 2017 11:41 AM

As mentioned by others, an important point about a DPO is that it is a role rather than a post and so can and often is fulfilled along-side other duties.
Having a named person taking the DPO role is important to ensure where responsibility for compliance is vested. It allows my clients to both respond quickly and appropriately to any data protection requests that are received as well as the act proactively to ensure compliance before any issues arise.

Whether DPO would have direct interactions with individuals depends a) on the size of the organisation and b) on whether the organisation has in place a mechanism and regular need to interact with individuals, such as a call centre. If such a mechanism exists I would expect common requests to go through that channel, for organisations with only infrequent direct contact with customers then having the DPO responding directly to requests should not be an overly onerous burden.

In terms of specifically listed benefits:

1) I agree, I think having a DPO ensures that data protection issues are raised as requirements during system and process design.
2) Possible, but I don't think this is a given.
3) I would see data security coming under a different role in terms of enforcement, the skills needed to provide and validate data security measures aren't ones I would see the person taking on the DPO role in my clients normally possessing.
4) An increase in quality and accuracy is likely to be more on a reactive than proactive basis I think, in that customers feeding that information being held is incorrect is likely to occur but I don't see a DPO coming in causing proactive data cleansing or quality management processes being put in place.

Posted by Tim M on 10 Mar 2017 7:59 PM

Our organisation doesn't have a specific job role for the DPO, our FD assumes the role of DPO within their remit.

It does make total sense for organisations to have a specific trained individual to look after data protection, I think it would be of benefit to our organisation to employ someone to assume the role even if it was a part time role.

I imagine the DPO would liaise with individuals but also with companies that I am sure will start appearing to work on behalf of clients for a small fee similar to what has happened with PPI.

I envisage the role if we were to appoint a dedicated DPO would have a positive impact on our organisation as there would be a single port of call for all enquiries and they could ensure a smooth resolution.

Potential benefits:

1) This would be a positive force within our organisation, Staff training will be key. One member of staff using To: instead of BCC: would be a breach in certain circumstances and it is important that they are advised appropriately and regularly (i.e. not one of training sessions once or twice a year)
2) I am not sure that having a DPO will directly affect/reduce the cost for individuals as that is stated in the GDPR whether you appoint a DPO or not.
3) If the DPO were to carry out regular spot checks and scrutinise in a constructive manner I feel this would be a great thing and also make people think. It would also be good for them to carry out a formal audit annually and report findings to management and the board.
4) Having a DPO would definitely increase accuracy and quality of data, it would also mean that there was someone to ask for advice and learn best practice from. It would also make people more assertive and lead them to scrutinise their own actions more carefully.

I think having a dedicated DPO would be a fantastic thing, I fear however that the role will just be placed upon an existing employee in many organisations for a small increase in salary to tick a box with little importance placed upon such creation of a role.

A5.2 Forum 2: Data portability (15-19 March 2017)

A5.2.1 Day 1: Introductions and Right to Data Portability

- Welcome to the forum! Please introduce yourself with your first name only, role and sector you work in. What are your data protection responsibilities in your organisation?
- What comes to mind when you think about 'data protection'? Please describe any word associations, images, feelings, examples that come to mind. Please upload any images, text or film to help demonstrate your opinions.
- Are you aware of the General Data Protection Regulation (GDPR)? If so, how are you aware of it?
- What comes to mind when you think about the GDPR? (E.g. its role, strengths/ weaknesses and perceived benefits)?

Posted by Aaron H on 15 Mar 2017 11:22 AM

Hi, my name is Aaron I am in the retail sector and have a responsibility for over 200 personnel members, each of which I have data protection involvement with. Also I am responsible for customer data protection. When thinking about data protection my role includes address, telephone numbers, NI numbers, DOB, bank details and credit checking info. The GDPR is something that I am aware of and believe that it should benefit EU citizensin protecting their details from dishonest overseas use. The main change is that it will make a "one for all" ruling, which should end any grey areas or uncertainty for everyone involved.

Posted by Philip N on 15 Mar 2017 3:07 PM

Philip. I work in the gaming industry as an Investigations Manager. I receive, vet and act upon data requests from law enforcement (police, immigration, HMRC, Trading Standards, NCA, etc) and retail outlets. I also request data from other retail outlet to assist in prosecutions. In respect of data protection it is a phrase which is used by the uneducated to block the sharing of data. The act was drawn up to assist and regulate data sharing, but people hide behind it. GDPR will assist in regulating data across the EU, but with article 50 being triggered it may become irrelevant and require single nation agreements. It will be good for the single complaint body, if and when it is set up. Also large fines will force companies to secure data.

Posted by Georgia W on 15 Mar 2017 4:11 PM

George, Deputy Manager, Hospitality.

data protection role is to protect the company data from attack or misuse from outside, and to protect client and staff data similarly.

Thinking about data protection calls to mind privacy and responsibility, it is easier for the equivalent of tittle tattle to go viral and do enormous harm. Also it is now possible for criminals to break in to held data records from a long distance, and to use the data fraudulently or worse.

Thinking about Data protection I imagine files left on trains, or strangers stealing passwords. It is concerning how much a stranger can steal if they use our identity. I do worry about tales where I hear that identity theft has been used to buy or sell anothers property. I don't feel that the loser in this situation should be the owner of the property/goods. financial institutions need to be more particular about verifying the identity of customers.

I am aware of the General Data Protection Regulation. But only hazily. I am afraid I really don't know enough about it to answer the last question.

Posted by Jess S on 15 Mar 2017 9:21 PM

Hello George, I was wondering if there had been much emphasis on data protection in your training in hospitality?

Posted by Georgia W on 15 Mar 2017 11:56 PM

Hi Jess.

No the organisation I work for is always a little slow to deal with modernity. I think many people within the organisation are completely unaware of the whole concept of data protection except in a vague way. Because I have access to many details about staff and customers I am probably more

aware than others in my org. But it is generally assumed that the way to deal with Data is just common sense...

Posted by Jess S on 16 Mar 2017 1:07 AM

Thank you for the reply George, I have never had any official training and agree I think it is just expected we use common sense.

Posted by Tony D on 15 Mar 2017 4:34 PM

I am Tony and I have data protection responsibilities for an online retail business. Data typically includes external customers' names and addresses and order information together with internal personnel details - the usual sort of stuff. I have been involved in data protection since the times of the first EU directive in 1995 which was incorporated into UK law through the Data Protection Act 1998, although it too the EU 12 years to realise that the Act did not in fact implement the directive fully. To some extent I think that the whole regime is a classic case of over-regulation. creating a vast bureaucracy which seems to be reactive rather than proactive in nature. There are a few high profile 'shock horror' cases mostly of large organisations' problems with cyber attacks or 'records being dumped in a skip' cases but when was the last time the majority of SMEs had any contact with the ICO apart from the annual demand to cough up the fee to keep the bureaucracy fed?

The GDPR is something that has been marching inexorable towards us for a couple of years and I first saw in in the Official Journal of the European Union in May last year. It consists of 99 articles (didn't quite make the three figures this time - maybe next time...) some of which are quite impenetrable. It is interesting to note that this time round the EU has decided to implement a Regulation which has direct effect rather than a lesser Directive which only comes into effect in a Member State when the State itself implements it (in the UK's case through an Act of Parliament of Statutory Instrument). Also interesting is that an individual's DNA is now included as personal data.

When the DPA first appeared in 1998 electronic data and the internet were both in their infancies with most data still being in hard copy. So I suppose the GDPR has a role to play in our increasingly paperless world but 99 Articles? Really! And whether a 'one size fits all' approach will really work is open to question.

Posted by Aidan S on 15 Mar 2017 5:24 PM

Hi, my name is Aidan, I'm a technical lead and I work for a software company.

- What are your data protection responsibilities in your organisation?

I am responsible for ensuring the team write and operate a secure service which ensures the confidentialty, integrity and availability of a variety of controlled data

- What comes to mind when you think about ‘data protection’? Please describe any word associations, images, feelings, examples that come to mind.

Fear, processes, procedures, ISO 2700.1, security state, surveillance, privacy

- Are you aware of the General Data Protection Regulation (GDPR)? If so, how are you aware of it?

Yes, it's something we will need to adjust processes to ensure compliance with in the near future

- What comes to mind when you think about the GDPR? (E.g. its role, strengths/ weaknesses and perceived benefits)

It has a clear rights based approach to data protection which helps protect individuals. Some organisations will find those more difficult to comply with due to aspects of their business model.

Posted by Simon E on 15 Mar 2017 6:27 PM

Simon, Commercial Director, online sales company. Responsible for setting guidelines on data protection within the organisation. Data protection involves names, addresses, email addresses, passwords, bank/credit card details etc. I am aware of GDPR bit not the full detail.

Posted by Rhiannon R on 17 Mar 2017 1:55 PM

Hi Simon,

Thanks for your comments so far. You said you were partly aware of GDPR - I was wondering what perceptions you initially had of it? Were they positive, negative or neutral? Why?

Many thanks,

Rhiannon

Posted by Oliver D on 15 Mar 2017 6:59 PM

Oliver, International Payroll Manager for a global high street and online retailer.

Data protection is something we already take great care and responsibility for and is governed by internal and group policy.

When thinking about data protection the thoughts that come to mind are responsibility, honesty, integrity and ethics.

GDPR has been discussed within my organization and a board has been set up to ensure compliance in all areas of our business. Due to the size of the business this is involving designated individuals from each business area.

I think generally GDPR is a good thing that will protect data but do have concerns with each member states SA treating this in very different ways which will lead to confusion and abuse. I am also keen to find out how this will play out with the UKs future around the EU.

Also i don't see how 'one size' will actually fit all.

Posted by Mark C on 15 Mar 2017 7:01 PM

Hi, I'm Mark a director in the retail sector....

I along with my fellow directors share responsibility for the data protection of our customers and staff...

I think data protection is fairly self explanatory but I do realize a lot of people are unsure of their responsibilities when it comes to knowing how to keep data secure and not open to abuse...

I educated myself on GDPR however our company did run a seminar on the subject..

It's a piece of European legislation that's due to take effect on 25/5/2018...

Posted by Rhiannon R on 17 Mar 2017 1:58 PM

Hi Mark,

Thanks for your comments so far.

Do you feel that your company were adequately prepared to teach its staff about the changes concerning GDPR? How easy did you find it to teach yourself about the subject?

Many thanks,

Rhiannon

Posted by Mark C on 19 Mar 2017 8:12 PM

Hi Rhiannon....It was not that easy to get hold of the full (lengthy) GDPR document but I have a friend within the European Commission that was able to help, but to dredge through the legal and moreover the contradictions was frustrating....

Our legal team was able to clarify the many queries I had but I would estimate that it took me a good 2 months to be satisfied that I was fully informed....

We are still working on the final training brief that will be rolled out in the coming month but the 3 test seminars we have held went well and highlighted the deficiencies in the information presented....

How is your company approaching the new regulations, are your preparations going well?

Mark.

Posted by Jess S on 15 Mar 2017 7:14 PM

Jessica, I am the Landlady of a village pub. Our data protection responsibilities have never really been outlined but from previous roles in the sector and retail I am aware of some of the legislation in place. I am responsible for ensuring my staff and customers data is protected from misuse. Data we hold includes names, address, bank details, NI numbers DOB and email addresses. Data protection is there to ensure personal details and information are not used for any other means than what they were collected for. I have little knowledge of GDPR and how it would be implemented in my business.

Posted by Russell W on 15 Mar 2017 7:35 PM

Hi I work for a finance company and have responsibility for employees and customer personal information. I look after information that includes names, addresses, financial and and security situations. Yes the GDPR helps unify rules for data protection eliminating loop holes and gaps in security across Europe and beyond. We were made aware by a course we had to take to learn some of the new rules. I think it is a good thing as it helps make things clearer for business and hopefully will give customers a piece of mind.

Posted by Beth T on 15 Mar 2017 7:40 PM

My name is Beth and I work for a well known high street Bank. I am a personal banker. My data protection responsibilities are:- *ensuring customer data is correct and up to date and ensuring opportunities to update are taken and recorded accordingly ensuring correct identification and verification has taken place *ensuring a "clear desk policy" is understood and adhered too to prevent breaches * to ensure confidential data is used and stored and disposed of in line with the data protection act * ensuring that correct identification and verification is adhered to for account openings and transactions *to ensure that company policy is adhered to with regards to our obligations under the data protection act. * to ensure that breaches are reported in a timely manner * to ensure staff have sufficient training in the subject area and that this is regularly tested and monitored with risks being identified and monitored Data protection - our responsibility to all living beings to be compliant with legislation and ensure that our company and all colleagues are aware of their responsibilities. It is our right to ensure that our data is used and stored correctly The new regulations will further reinforce the current regs but make companies far more accountable for breaches and will help to ensure that breaches are heavily penalised. I am aware of this as we have been given a brief over view of the main points, main changes and how it will affect us

A5.2.2 Day 2: Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. (ICO)

- How does the situation in respect of data portability under the GDPR compare with the current situation (DPA)?
- Do you envisage the right to data portability to enable your organisation to acquire and use more/more detailed data on individuals *who provide data* to your organisation?
- Do you envisage your organisation to be able to use more/more detailed data on individuals to *improve the service* provided by your organisation?
- How important is this right for enabling consumer confidence relative to other sources of consumer confidence (such as a track record of data security, brand reputation)?
- What proportion of your customers/data subjects to you expect to exercise the right?
- How big a problem is inconsistent/out of date personal data?
- Will the right to data portability improve the consistency of data?
- What is more consistent data/access to data worth to your organisation?

Posted by Aaron H on 16 Mar 2017 12:25 PM

The changes in legislation should make it easier for the consumer or supplier of data to move their details almost seamlessly between organisations. I believe that the right to data portability will enable my organisation to acquire more detailed data on individuals who who provide data to my company. We will be able to provide better financial services to customers who use this. The importance is high as customers will know what information they are sharing with us. Unfortunately I feel that the proportion of customers using this will be low due to lack of knowledge of it. Inconsistent and out of date personal data plays a large part in declined credit checks so it can be a big problem. The right to data portability should increase the consistency of data however it will be down to public awareness. The worth of consistent data and access to data is massive to my industry, however it is only validated by how many people agree to it.

Posted by Rhiannon R on 17 Mar 2017 2:09 PM

Hi Aaron,

Thanks for your comments so far.

In what way do you feel you'd be able to provide better financial services to your customers who exercise their use of data portability? Do you think there would be any price reductions as well as service improvements?

You also mentioned it's down to public awareness - how well do you think rule changes will be promoted to the public?

Many thanks,

Rhiannon

Posted by Aaron H on 18 Mar 2017 10:57 AM

Hi Rhiannon The improvements would mainly be around being able to correctly market the right products to suit the customer, customers can become alienated and lose trust in organisations who mis-market them. Up to date data is then vital to provide the best possible data. With customers being able to port their data quickly and freely there could well be an increase in competition for business which in turn would lead to price reductions or better terms. In relation to public awareness I believe the rule changes will be well publicised through the media.

Posted by Tony D on 16 Mar 2017 3:39 PM

1) There is currently no concept of data portability under the DPA. The GDPR introduces the concept although not named as such in Article 15. The idea is that a data subject can request transfer of their electronic data from one controller to another without hindrance. However the right of portability is limited by the phrase 'technically feasible and available' in the Article so expect plenty of hindrance. As is common in EU affairs it is recognised that there are significant differences among Member States about the right. The growth of electronic data use since 1998 when the DPA was enacted means that the need to transfer such data between controllers is likely to become more important but probably not easier.
2) It is unlikely that my organisation will require any further information from a customer over and above that already given.
3) It is unlikely that more detailed data would improve the service already given as data usually given is sufficient.
4) I should imagine that most, if not all, customers/data subjects will be aware that the right even exists let alone what it means. So I think that it will be very unimportant in consumer confidence. In my experience consumers are only interested in whether the organisation can fulfil the contract quickly and efficiently with simple rectification if things do not run smoothly.
5) I do not expect any of our customers to exercise the right.
6) Out of date data is not a problem with our organisation as data is regularly cleansed. Generally it can be a slight problem - I still get mail addressed to me as secretary of an organisation; a role I relinquished ten years ago.
7) It is unlikely that the right will improve consistency for the reasons given in 4. above.

8) The data that we get and use at the moment is sufficient for our purposes so the worth of more consistent data would be negligible.

Posted by Philip N on 16 Mar 2017 3:59 PM

The right to transfer data does not, on the face of it, present any new challenges as our customers already do this and certainly within the financial services and banking industry this is now the norm. Data portability will certainly assist in the creation and maintenance of accurate and up to date data sets. It should also prevent customers attempting to create multiple new false accounts. Improved levels of service is one of the best possible outcomes as in the event of a breach we can ensure that co fact with customers is swift. Customers can also be better targetted during directed marketing campaigns. Brand reputation is everything and anything which will heighten levels of trust and integrity has to be welcomed. Due to recent high profile 'hacks' the percentage of customers looking at this is considered to be high, however, it depends on how informed they are and how well this is communicated. Out of date data is a big problem, not only for customers trying to verify accounts, load and unload funds, etc, but also when data is requested by law enforcement or courts. Incorrect data provided in the latter circumstance could lead to significant brand reputational damage and legal challenge. Also bad data in respect of retailers can lead to bad debt and contracts signed by persons no longer engaged in the business. Portable data should improve the situation, it only if it is correct in the first place. That said additional checks at the point of transfer will remove /reduce this problem. Consistent and accurate data will lead to seemless process and a reduction of the requirement to risk assess customers at the highest level and the introduction of delay in purchasing / wagering. Customers want a seemless transition and minimal delay when setting up new accounts.

Posted by Mark C on 16 Mar 2017 9:24 PM

I think that the current system is less restrictive than the new system appears to be, however this remains to be seen....With new technologies and cloud storage systems being introduced, i.e. new machine learning and data analysis tools (Big Data etc.), my concerns may well be premature.

The data we currently use can be retrieved and analyzed in more and more inventive ways and this data will enable us to be more competitive across our operations.

We already have a good data security history which can be researched and supported by industry professionals and commentators alike.
Our brand and reputation among our customers is high and we measure this satisfaction on a regular ongoing basis....Currently less than 2% of our data subjects request a report on our data security history however I expect this to rise on the implementation of GDPR.

We have some real problems with out of date data and we envisage the introduction of machine learning to assist us in mitigating those problems and we envisage no problems arising from data portability.

More consistent data/access to data is, like any company I would expect, is priceless...

Sometimes I yearn for the old days when everything was paper based and you just locked it away in a filing cabinet....Then I remember how we used to struggle to collate and present information, so thank god for the internet and technology....

Posted by Georgia W on 16 Mar 2017 9:29 PM

AS I understand it the data portability is not considered in the DPA at the moment. It obviously does happen a bit in some organisations. Ie I feel that the gov.uk already has parts where they can link data across different departments (passport photo - drivers licence/ information about insurance to road tax..) Mostly at the moment we all re-enter data over again whenever we start to deal with a new online company.

The data information which my organisation holds on people(guests/staff) is fairly simplistic stuff and I don't at the moment envisage us using this to aquire more detailed data, because then we would have to store it. and if we don't need it that would be a waste of time, space, staff and security effort.

I think I have just answered the third point above, I don't, at this moment, envisage using more detailed data on individuals to improve the service provided by our organisation although , now that you have raised this as a query it makes me wonder whether it wouldn't be worth having a meeting to see if there were any data which we could use to improve the service, in addition to the data we already try to collect for this. My gut feeling is that we are limited by size, staff and funds as to what tailored services we could introduce as a result of any data analysis anyway.

Many of the customers who presently use us are generally older and fairly innocent of any concepts of data collection/ management etc. We even have a small subset who do not even use computers. I don't think at this moment in time any users would query how safe their data was with us. It is possible that the staff might be more concerned about portability of data.

I certainly believe that the right to data portability should improve the consistency of data , don't forget though that this means that if data is inaccurate or false this also might get reproduced throughout the system.

Because the organisation I am part of is rather niche in its specialisation and organisation I think that although this data is potentially useful, I believe the value at the moment is only moderate.

Certainly in the near future I do not expect any of the customers to exercise this right certainly within the first 2-4 years..

Inconsistent and out of date data is not usually a problem to us as because we are quite a small part of a whole, and when people need to give us specific data we can phone or write to them for information or clarification. We are in quite a strange and unusual place for an organisation though.

Posted by Jess S on 16 Mar 2017 10:07 PM

I have not come across data portability under DPA. The right to data portability would improve the service of my business. By having more details of customers I can offer different services tailored to the information I receive. I think having a good track record in data security is very important, we adhere to the current DPA but I don't think our customers would put our business and data security in the same sentence. If we started to collect more data then I would place more emphasis on ensuring customer confidence. I don't think many people are aware of data portability at the moment so few will excercise the right. Out of date personal data is not a problem for our business more of an inconvenience. Many of our customers are local and known to us. Consistency of data will improve in the long run and with more people being aware of the right. A system that gives customers an easy way to transfer data and for the companies to receive it will only benefit us. Collecting data can be time consuming and expensive for a small business with limited time to spend on this area. My only concern in obtains the dat would be the cost to our business.

Posted by Rhiannon R on 17 Mar 2017 3:42 PM

Hi Jess,

Thanks for your comments so far.

It's interesting you say that data portability could help you offer more tailored services to your customers - what specific improvements do you envisage? Do you think there could be any price reductions for customers, as well as improvements to the service you offer?

Thanks,

Rhiannon

Posted by Jess S on 17 Mar 2017 9:59 PM

If we can capture more detailed data, for example marital status number of dependents we could tailor events towards the majority. For example intimate dining experience to family fun days. I think there could be price reductions if the data showed a need for it and would benefit our business. I think in general it would help us promote different offers.

Posted by Aidan S on 16 Mar 2017 10:27 PM

Standards for data portability to support this right will greatly improve my companies ability to operate by reducing data acquisition costs. In most organisations I'might familiar with the change in approach this right forces will be very alien and require a lot of systematic change to support

Posted by Rhiannon R on 17 Mar 2017 3:44 PM

Hi Aidan,

I'm interested in how the change in these standards compares with the current situation (DPA)?

You spoke about 'systematic change'... what do you envisage being the biggest changes? What will be the most and least beneficial changes as a result of this, in your view?

Thanks,

Rhiannon

Posted by Russell W on 17 Mar 2017 4:49 PM

1) I feel it makes it easier to transfer data seamlessly across global platforms under the GDPR. At the moment it is hindered by the current rules and regulations.
2) I suppose the data could prove more useful in the future but at the moment I cant see where the extra information would benefit my company.
3) Parts of the data regarding financial situation may be of some extra use in providing a more targeted service to our customers. We still hold a moral right not to abuse this and to do whatever is in our customers best interests.
4) This is very important, our customers trust us and the fact that we can protect our data and not abuse it ourselves. I hope our customers will see the benefits of the new rules but I guess most of them will trust us as we have a good record in this area.

5) I can not see any of them doing this as they choose us and trust us. Many will not even have an idea of what the new rules /rights entail.
6) It can be a big problem, especially when trying to be efficient in the way we deal with our customers. Any delay can be expensive to both us and our customers.
7) I think that data consistency will improve as we are more easily able to obtain the right data.
8) It is worth a lot as it enables us to work better for our customers thus gaining more custom and growing profits.

Posted by Oliver D on 17 Mar 2017 7:47 PM

- There isnt really anything in the DPA relating to this but i don't feel this has been adequately covered in the new regs. Will individuals really be bothered to request this? and will this actually increase trust? Also how can 'technically feasible' actually be defined.
- In my area the data that is collected is used to protect, help and aid contactability of an individual therefore i don't see there will be a need to collect extra data
- More data will be irrelevant to the service provided in my area but surely this will lead to misuse in many instances.
- I doubt people will actually be aware of this, and if they are, will probably not fully understand the implications
- I dont expect anybody to
- If we hold out of date information in my area we would not be able to pay individuals on time. We therefore encourage individuals to keep their data accurate themselves via self service portals
- No, i feel it will cause conflicts until it is at a point where it is truly effective
- It will benefit our employees but ultimately is the individuals responsibility

Posted by Beth T on 18 Mar 2017 7:07 PM

Currently personal data has to be requested, at a cost and will only be provided in paper based form which can delay and hinder the customer experience. The ability to transfer and reuse electronically will speed up transactions and requests. If the ability to do this is guaranteed to be safe and secure it will really enhance the customer experience and customer confidence If customers are happy to provide us with this data and are agreeable to it's subsequent use, I am sure that it may enable our organisation to tailor our products and services on a far more personal and individual basis which in turn would enable us potentially to improve our services to individuals. It is obviously important that individuals and consumers have confidence in the security of their data as this will increase their brand loyalty As many as we are able to reach out to! Out of date data / inconsistent data has been a big problem for us but we have introduced a series of software updates which prompt us to request, confirm and update customer data at point of contact. Customers are able to update their own data on our online system. I'm not certain whether it will improve the consistency of data as it will still only be updated as and when customers choose to inform us. I'm sure it will be valuable to our organisation as holding the correct data is going to increase productivity and improve the customer experience

A5.2.3 Day 3: Right to Data Portability (2)

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. (ICO)

1) Do you expect people to switch away from or to your organisations?
    1) What percentage of your current customers might be susceptible to switching to another provider?
    2) What percentage of customers might you be able to gain?
2) Have you taken any steps to make the personal data you hold more portable in anticipation of GDPR? What did that cost?
3) For what type(s) of data would portability be most valuable and why?
4) Do you expect to use more personal data that was originally collected by other organisations as a result of data portability?
5) How many items of personal data do you hold per person / require users to provide?
    1) What type of data?
    2) How often is this collected?
    3) Do you use observed / monitoring data?
6) What proportion of that data exists already and could be ported from elsewhere (i.e. that doesn't need to be created from scratch)?
7) How long do users take to input their data?
    1) What fraction of that could be cut if data were portable from another service/provider?

Posted by Aaron H on 17 Mar 2017 10:15 AM

I don't believe people will necessarily switch away from my organisation as most of the data we keep benefits them for direct marketing and offers, it would therefore be almost impossible to quantify percentages of loss or gain. Steps have been taken within my organisation to help with the portability of personal data however I wouldn't be able to specify how far along the journey is or the cost. Recieving chunks of customer shopping profiles i.e. Spending habits and frequencies along with contact details would be invaluable to profile customer wants and needs. I do expect we will be using more personal data collected by other financial services as it will speed up customer experience. Depending on the services we provide we hold varying amounts of data per person, on average we hold name, address, DOB, email, this is usually collected from the user them selves at point of sign up. Past this point we collect data every time we have an interaction with the individual and monitor their activities both on line and in store to build up a profile of them which assists us in marketing the best propositions for them. The data we use would already exist and could be ported from elsewhere however the time taken to collect and input the basic details we collect is minimal so the time saving would be so also.

Posted by Tony D on 17 Mar 2017 3:24 PM

1) I don't think that the right to data portability will encourage people to switch way from my organisation. The data that they give us is used primarily for shipping orders and for direct marketing purposes. I would think that the numbers seduced by other organisations and those we could lure away from others *because of the right of portability* would be less than 1%.
2) The only steps taken are to write a few SQL scripts, but until the EU decide upon and flesh out the technical requirements of portability we will be in the dark as to what the common interchange format(s) will be.

3) I should imagine the most valuable types of data would be simple personal information and, more particularly, for industries where switching between providers is encouraged, such as energy providers, and, in the future, water companies.
4) I do not expect to use more personal data originally collected by other organisations. The data that we need to use is relatively simple and straightforward to collect.
5) Typical data collected are name, address, telephone, email and products required. For staff there is DoB, next of kin and pay rates etc. Data are collected when orders are placed which is constantly during the day and evening or whenever staff are recruited etc. We do not use monitoring data.
6) I should think virtually all data (>95%) we use already exists. Very little is generated from scratch.
7) It does not take users very long to input their data - a matter of moments. Consequently the time that portability would cut would be negligible.

As I noted yesterday, I doubt many people will be aware of or understand the significance of the right so the opportunities it will present will be very limited.

Posted by Rhiannon R on 17 Mar 2017 3:48 PM

Hi Tony,

Thanks for your comments so far.

You've mentioned a couple of times that you think few people will understand the right to data portability in its full significance - do you think understanding will improve over time? Do you think in reality the advantages will help the organisations it affects more than consumers? Why/why not?

Thanks,

Rhiannon

Posted by Tony D on 17 Mar 2017 9:40 PM

Hi Rhiannon

I doubt that understanding of data portability will improve over time. I think that the vast majority of people will be not interested in the concept as it is abstract in nature and it will not be something they would think about using regularly, if at all. Identity theft has been very much in the public eye recently and people are told to be very selective about what personal data they share with others online. This is likely to have a chilling effect on the usefulness of data portability as people will become more wary about giving others permission to access their data.

Also the complexity of the GDPR inspires neither confidence nor clarity and I doubt that the Government will consider data portability to be a priority for a public information campaign. I would suggest that consumer rights legislation is more important to the general public in their day-to-day lives yet there has been no public information campaign about those rights in general or to the recent changes to the Distance Selling Regulations in particular.

I would think the advantages, if any, will help organisations more than consumers as the concept would, in theory at least, allow organisations to achieve quicker assimilation of data as manual transposition would not be required so eliminating keying errors and improving data

accuracy However, consumers have become used to keying in basic data such as name and address, the latter beings often automated through postcode lookup, so I think any advantages for them would be minimal.

Hope the above answers your questions.

Regards

Tony

Posted by Rhiannon R on 18 Mar 2017 2:17 PM

Thanks Tony - very interesting!

Best wishes,

Rhiannon

Posted by Russell W on 17 Mar 2017 4:59 PM

1) I can not see our customers switching at all as they are happy with our services and many , like we see in the banking industry just can not be bothered to switch. In the same way I can not see us gaining many customers either because of this.
2) At the moment we have not taken any steps bar assessing our security systems. We know more portable data can lead to security riskd and have spent Thousands in getting systems in place to combat this.
3) The most valuable data would be personal information as it is the information companies need most, its the customers that are important after all to any business.
4) At the moment I can not see us using extra personal data, more likely we will work hard to protect what we already hold.
5)
    1) names , DOB , address , financial details, credit history and assets.
    2) revised yearly.
    3) we monitor data to protect it in a secure manner.
6) I suppose 100% of data already exists but it is much easier to create from scratch as we can trust the data more. We also want to create a picture we can trust and not rely on potentially corrupt data.
7) Users are efficient in inputting data as it is a necessary in our product. That said other providers would not be a secure source of information so it would be hard to trust this anyway.

Posted by Oliver D on 17 Mar 2017 8:00 PM

1) The data we hold is used to be compliant with legislation and to pay individuals and therefore is used for their benefit. This therefore is not applicable in my case.
2) No but this is being reviewed in other areas of the business
3) Probably personal details which can be used for marketing.
4) No, we do not need increased data, also employees would see this as questionable. We would therefore seek to increase protect of the data we hold

5) Personal data, job history, pay rates, account details. Standard payroll/HR related. This is collected upon joining the company and updated as needed, for example when an employee changes bank account or a pay review is conducted.
6) We would need the individual to supply the data so we can ensure it is accurate. For example if account details were received from elsewhere how could we be sure it wouldn't be fraudulent. Where would supporting evidence come from?
7) Not very long but as long as it takes as it is in their benefit to process this (in my situation).

Posted by Jess S on 17 Mar 2017 10:01 PM

I don't expect people to switch from us as we are convenient for many of our customers and data portability will not change this. If data portability provided us with more data of consumers which I believe it will then we might hopefully gain some customers. Regards to a percent I'm sorry but I just don't know. We have not made any steps in anticipation of GDPA as we just don't know enough about it. Contact details, DOB, marital status, number of dependents and age, spending patterns, salary, ethnic origin would be beneficial to us. We could create a profile of the individual and cater events towards this, for example if lots of the data showed customers with children we could provide entertainment for the children to encourage the parents. If we could estimate an average salary we could reflect this in a our pricing. I am expecting to use more data that was collected by other organisation. As I have previously said we don't have the man power for emphasis on data capture so it's great the work will have already been done for us. Staff data collected includes name, DOB, address, email, NI number, telephone number, bank details and next of kin. Collected on employment. Customer data is generally name, email address and telephone number. This is collected when booking with us. We don't use observed / monitoring data. All our data is created from scratch. To input data only takes a few minutes, most of our data is captured over the telephone taking a minute. I don't think importing would take any less time due to the limited data we capture.

Posted by Georgia W on 17 Mar 2017 11:23 PM

Our organisation doesn't have any immediate like for like rivals so I'm not sure that I expect any great change in customer base, (apart from the fantastic upsurge that is bound to happen as a result of my marketing and adminitrative skills; ho,ho..) So there is no percentage of customers who might switch to another rival because there isn't one. Like wise portability of data won't affect the number of customers we could gain.

We haven't taken any steps to make the portable data we hold more portable in anticipation of GDPR, so there has been no cost. As a result of this forum I am going to raise the issue with others in my organisation but I expect after some meetings, we will be issued with a notice that will summarise what GDPR is and what we should expect to do about it as far as our ability stretches (which will probably be found to be small.)

I'm really not sure for what types of data portability could be most valuable. If any. It is more useful and less valuable? to us. I know that one can put a price on everything but in relation to my organisation, the data is more of a necessary tool and less of a cost/profit?

I suppose if portability gives us more data then we will probably be able to make use of it. We hold fairly small amounts of data per person, although many people come in groupings. People don't always remain in the initial grouping and can move from one to another.

We hold personal data, financial data, adresses (both home and work and including email), employment roles, voluntary roles, racial and ethnic profiling, gender, age, health, dietary and medical data.

This is collected when guests use us. this can be several times a year, once a year or intermittently. The same is true for staff.

We do use low level monitoring/observed data to make sure we supply and provide correctly for peoples personal needs.

I suppose about a third of the data exists already and the rest is more specific to our organisations needs. If this could be ported straight over somehow I guess that would be good, but as I say,- a lot of our organisation is fairly behind the times and I imagine this wont be easy for a few years.

I don't think it takes that long to input users data , we don't have pages and pages of forms like the DHS or something, we only need a two sided form and some of that is information we want to be sure the users have received..

Also we have holes in our data where we deal with people who we might hold very limited data on, eg, name, financial data, home address phone number maybe email.I suppose portability might help us to flesh out these occasional bones..

Posted by Beth T on 18 Mar 2017 7:28 PM

I do not think that the change will encourage customers to switch organisations unless a breach of data occurs within their existing organisation which reduces consumer confidence. We have introduced new software within our customer contact areas (face to face and telephone) which enables colleagues to request data updates and provides management with information as to whether colleagues are using or choosing to avoid. The website has had security enhancements which also enable customers to update their information. I am not aware of the cost but do know that this area has been heavily invested in Portability would be important for the data that is most often required. We may be interested in what information competitors hold relating to products and services and the customers reasons for selecting these. Full name, marital status, dob, country of birth, country of residence, country of nationality, tax status (Fatca) NINO, marketing preferences, employment status, employer details, annual income, expenditures, number of financial dependants, contact details, current and previous address This data is updated / monitored on the majority of occasions that we interact with customers and taken in full when creating profiles for new customer. This data could easily be ported from other organisations that already hold it. This would reduce transaction time and allow colleagues es and customers more time to deepen relationships and obtain better service

Posted by Mark C on 19 Mar 2017 8:28 PM

I envisage most people will not be that bothered about moving their data, certainly individuals, businesses however are a more unpredictable beast.....Certainly many of them will be looking to migrating their information and this area is an opportunity for us and our new business model. I anticipate and would be satisfied with a 5% increase in customers but this is my figure, my MD may well think differently!

Our IT director tells me that we have A thorough worked and tested strategy for the anticipated roll out and we are in an excellent position to fully enable portability across all channels.

Companies that wish to monetize your data or create value (like using your social graph to personalize an experience), will benefit not from owning your data — as so-called "walled gardens" of the past have tried to — but rather by cultivating a relationship with you — one in which they have persistent access to you. The consequences of this way of thinking are profound. Instead of the hostility that comes when users are locked in, it encourages innovation and superior service to ensure that the flow of data doesn't close off.

Companies can also get a bigger piece of the data pie when embracing portability. If web services could assemble as a "federation" based on trusted data exchanges, they could get access to more timely and relevant data than they otherwise would on their own. The pie is bigger and everyone benefits.

We currently hold data such as, but not limited to, Names, address, card details, average spend, visiting history online/offline, purchase history etc....All of this data is now collected and collated in real time...

A5.2.4 Day 4: Fines

Under the GDPR, supervisory authorities are empowered to impose significant administrative fines on data controllers and data processors. Maximum administrative fines of up to €20,000,000 or (in the case of undertakings) 4% of global turnover can be imposed for infringements of the basic principles for processing, including conditions for infringements of consent (Articles 5, 6, 7 and 9); data subjects' rights (Articles 12-22); the rules on international transfers (Articles 44-49) and others.

1) Do you envisage that an increase in the severity of fines for failing to protect consumer data would lead to your organisation taking data protection more seriously? Why or why not?
2) Have you taken / do you expect to take any additional security measure in response to the increase in maximum fines for data breaches?
3) Do you envisage that an increase in the severity of fines for failing to protect consumer data would increase the willingness of individuals to provide personal data to your organisation? Why or why not?
4) How, if at all, will this benefit your organisation?

Posted by Aaron H on 18 Mar 2017 11:05 AM

1 My organisation already has strict rules and guidelines in place so I wouldn't say we would be taking it anymore seriously but the increase in fines and changes in legislation will mean that all involved receive some form of training, especially as the onus of proof of consent will now lie with the organisation. 2 The additional security measures that will be involved will be focused on web site security and additional internal audit compliance checks. 3 As long as public awareness is raised then I think individuals will be more willing to share data with my organisation, the knowledge of the severity of fines for companies not protecting individuals data would strengthen their confidence. 4 The more readily people share their data with us the easier it is for us to map their journey with us both on and off line, this would give a more comprehensive view of the customer meaning we could tailor both their web experience and any marketing to them.

Posted by Russell W on 18 Mar 2017 3:33 PM

1) We already take data protection very seriously but have obviously sent our staff on courses so we know the new rules. Our customers rely on and trust us to protect their data so we already take this very seriously.

2) We already have tight controls over access, anti hacking and anti virus softwear. We will remain just as vigilant as ever.
3) Our customers already have immense trust in us due to our track record. The new measures will add extra piece of mind but many of our customers may not even know of the new rules anyway.
4) This just underlines the importance of data security, it re-enforces to our staff the importance of correct procedure.

Posted by Oliver D on 18 Mar 2017 3:54 PM

1) Yes i believe this will encourage data to be taken seriously but all steps will be taken to ensure it doesn't happen. My company would not want this type of fine to be known publicly as it would lead to a diminished brand view and potentially reduced sales.
2) We are working towards ensuring we are compliant but not because of the fines, this is more around ethics and giving employees and customers trust around their data.
3) I don't feel this will increase the level of data provided to us as the public will not have faith/trust in this system, if they are aware of it at all, and increased data will be irrelevant to us.
4) It will not benefit us as we already treat data very seriously, this is covered in policy.

Posted by Beth T on 18 Mar 2017 7:44 PM

We already take data protection very seriously and are compliant in our collection and storage. We ensure our staff receive on going recordable training and assessments in this area and have management data which collects information on individual colleagues data capture during customer transactions. I am certain that our organisations will increase the daily monitoring and what is captured. I am sure that colleagues who chose not to update will face serious consequences. I do think that customers will want to know that their data is being stored safely but I doubt that many will realise the severity of the consequences for the organisation not complying. Some customers are willing to update their information whereas others feel that our request to update and monitor their data is a bit "big brother" If customers were aware of our obligations and the consequences of non compliance I am sure that the majority of them would want to ensure that their data was up to date but there will be some that really won't care less as they think it doesn't effect them!!

Posted by Tony D on 18 Mar 2017 9:27 PM

1) The present maximum fine that the ICO can impose is £500,000 and has been so since 2010. However, the latest statistics from the ICO for quarter 3 show that it issued just one fine for a data breach during the quarter. That was in a case where an employee of an historical society had an unencrypted laptop containing details of donations to the society stolen while working away from the office. The fine? just £500.

   For 2016 as a whole there were 237 incidents reported to the ICO where emails were sent to the wrong recipients and 76 incidents of failure to use bcc when emailing.

   My organisation already takes data protection seriously but I don't think the increase in fines' severity will result in any change in procedures. The current maximum fine is a big enough deterrent for most SMEs and any increase will be academic for all but the largest organisation. For the ICO to fine an organisation so much that it would be bankrupted would be both disproportionate and counterproductive as it would be seen as heavy-handed. The problem at the moment is that the ICO is reactive - it will only take action if something is reported to it and that action appears to be more carrot that stick. For the majority of

cases the ICO seems to be keener to use the 'carrot' of getting signed undertakings from organisations to improve procedures rather than the 'stick' of financial penalties.

Of course for very serious data breaches involving the loss or misuse of large amounts of personal data the increase in fines will be significant to the type of organisation that can afford to pay, such as banks, *but only if the ICO chooses to impose the larger fines*. These large organisations have data on many thousands or millions of data subjects although the damage to the organisations' commercial reputations from adverse publicity about data breaches will probably be more of a concern to them that any financial penalty.

2) We have not taken nor do we expect to take any additional security measures in response to the increase in penalties. Data held is already well encrypted and staff are regularly reminded about the importance of data security. There is little more we could do in practice to increase security that would be proportionate. That is not to say we are complacent about the importance of data security - far from it.

3) I do not expect that the increase in severity of penalties will, in itself, increase the willingness of individuals to provide information to my organisation. I doubt that many people will even know what the penalties are and, in any case, I would expect there will be an increasing 'prevention is better than cure' attitude as people are always being told to be wary about what data they share. For individuals any fine imposed on an organisation would not compensate them for any loss or inconvenience they might incur from a data breach or loss.

   It is in the nature of people to provide such information as they think is necessary for them to achieve their goal, for example to buy a particular product. If the website seeks too much data the individual is likely to simply give up and go elsewhere. We ask for and consumers need to provide us with only basic data most, if not all, of which can be found from other sources and we do not retain any credit or debit card information that is provided. Staff information is held on standalone computers and access is strictly limited.

4) I presume that the 'this' means the willingness of individuals to provide data. There may be some benefit to us if the individual is minded to provide more data that can be used to understand their buying habits to target future marketing. But as stated above I think the increasing awareness amongst internet users to limit the availability of their data will negate any willingness to provide more data than is necessary to achieve their aims.

Posted by Jess S on 18 Mar 2017 9:40 PM

The increase in the severity of fines will make data protection more of a priority in our business. As a small business we cannot afford to lose money on fines. Once we have fully researched the GDPR I envisage we will have to put additional security measures in. If GDPR becomes common knowledge I do think individuals will be more willing to give data to our business, I think any measure which shows that companies have to improve data security gives the consumer more trust. If data becomes more available and is cost effective in obtaining it, it will benefit our business. We can tailor our products and events to different groups in society. Although we are aware of our immediate consumer base it would be beneficial travel further a field.

Posted by Georgia W on 18 Mar 2017 11:24 PM

My organisation can be slow to engage with outside legislation. I would hope that these fines may make it take data protection more seriously, but unfortunately the whole organisation has a presumption that it is special and normal rules don't apply. It is also slow to process change.

I would imagine that we will take additional security measures, you can be sure that as a result of this forum I shall be lobbying hard to find out the answers within my organisation to these questions for my own sake.

I do expect to take extra measures by satisfying myself that sufficient measures are in place to prevent such breaches.

I am not sure that most of our guests are savvy enough to be aware of these new rules, so I doubt that this would have any bearing on the amount of data that they might be willing to provide. The staff may feel more reassured but aas they would mostly have to provide this data in order to benefit from the employment then I also don't think it will affect the amount of Data that they provide.

I think that there will be null effect to my organisation overall. Although perhaps our data security might be a bit higher.

Posted by Mark C on 19 Mar 2017 8:36 PM

We already have more security than we really need, so I can't say my company would take data protection more seriously as we already have a stringent, non negotiable approach to data security embedded in our company practices.

We have a good record for data security and most of our customers and trading partners understand this so I think our customers may be more reassured by the new fines available but they won't necessarily be any more or less likely to share their data....

A5.3 Forum 3: Data access & erasure (15-18 March 2017)

A5.3.1 Day 1: Introductions and Right to Data Portability

- Welcome to the forum! Please introduce yourself with your first name only, role and sector you work in. What are your data protection responsibilities in your organisation?
- What comes to mind when you think about 'data protection'? Please describe any word associations, images, feelings, examples that come to mind. Please upload any images, text or film to help demonstrate your opinions.
- Are you aware of the General Data Protection Regulation (GDPR)? If so, how are you aware of it?
- What comes to mind when you think about the GDPR? (E.g. its role, strengths/ weaknesses and perceived benefits)?

Posted by Anna T on 15 Mar 2017 11:06 AM

1. ANNA 2. Data administrator; protection of student data 3. Education section. 4. Data protection is a legal requirement, ensures safety, authenticity, accountability 5. GDPR: i am aware of GDPR only as another variation of the plethora of legal requirements regarding data protection 6. GDPR attempts to enforce more data security but how much of an impact it has made in practise within the education sector i am unsure

Posted by Gill K on 15 Mar 2017 12:08 PM

Gill

Administrator - Legal Profession.

Data Protection - to ensure Data is kept secure at all times.

Data needs to be protected, from not leaving information lying around to ensuring computers are secure, and on going problem for a lot of organisations.

GDPR another raft of legislation but will it be valid after the UK leaves Europe, if it ever does, can?

GDPR a lot of new words and detail to absorb, which is very difficult for small companies on tight budgets, who do not have a specific data protection department.

Posted by Cymro J on 15 Mar 2017 12:10 PM

Hi ... Cymro, Management Information Officer for a national 3rd sector organisation. Data Protection = Privacy, security, consumer rights. It's a legal requirement on organisations that keep data on you to ensure that the data is held securely, the data is accurate, you have given your consent, they can justify the reason for each piece of data that's kept, that it is only kept for the length of time in accordance with consent or the reason why the data is kept. The GDPR gives consumers and users of services greater control over what personal data is kept on them, greater rights over accessing that data and of withdrawing consent. It places stricter deadlines on the access to data (Subject Access Requests etc). If the organisation is rigorous in it's application of the current DP act and follow OCO guidelines the GDPR will still have some impact re building capacity to respond more swiftly to data requests.

Posted by Barbara D on 15 Mar 2017 12:45 PM

Hi, I am Barbara, I am COO and Compliance assistant and I work in the financial sector. I am responsible for the data protection in our organisation and I am assisted by a compliance consultant. We are a small B2B firm and we deal with a limited amount of personal data. Data protection is a legal requirement, data must be kept safe at all times; a safe is the image I associate with data protection. I am aware of the GDPR because I must have read something online (professional/industry/compliance websites/blogs.. I don't remember). I only skimmed through the what's new section but I really need to get much more information.

Posted by Judith B on 15 Mar 2017 1:09 PM

Hi I'm Judith and I am the Record Services and Archives Manager for an emergency service. My department are responsible for subject access requests and I am repsonsible for the records for the whole of the organisation. My role revolves around DPA.

DPA to me as about protecting the information that we hold within the organisation on any individual. External or internal. My responsibility is to protect the organisation's data and that of our clients. I need to ensure that everyone is protected appropriately.

GDPR is a change to the DPA legistlation and new rules will come in to play in Qpril 2018. The new rules will impact on the way by department deal with SARs. Within my department we currently have a role which is dealing with GDPR, it's roll out and the implications for the organisation.

GDPR will change a number of things from a subject access perspective, fees, time to respond etc but it will also mean tougher penalties and more restrictions which in turn, I believe, protect data.

Posted by Nigel B on 15 Mar 2017 7:22 PM

Hi I am Nigel. A project Manager for a Business consultancy working in Major projects such as HS2.

One of my roles is data protection for the company where it is mainly about our clients data.

data protection is applied at many levels in our organisation.

1) Our own personal files and client names and addresses at the basic level.
2) Similar data from clients when we are involved is advising TUPE programmes.
3) Distributing client data to our associates for use in workshops and quotes / bidding for work.
4) Ensuring all data and emails are "safe" when on Laptops, phones and tablets in all circumstances.

I have looked at GDPR since it as started to appear as a requirement in major project PQQ's and ITT's as a possible requirement for next year on the projects I work on which may last several years and take 6-24 months to finalise and start.

It looks to make things more encompassing. It lacks a focus. more aimed at social media and not a working environment

Posted by Linda C on 15 Mar 2017 7:23 PM

Hi, I'm Linda and I am Head of Data in a global B2B organisation. I am responsible for the governance and security of customer information.

Data protection to me means safeguarding the information customers have provided and ensuring it is used in a responsible and agreed way. This is becoming increasingly difficult in a 24/7 digital world with employees hot-desking in flexible locations, and I think companies have to be as vigilant about potential unintended breaches as the deliberately malicious ones.

I am aware of GDPR through various newsfeeds, supplier briefings, and now our legal team have engaged a law firm to steer us through it.

I can foresee a lot of work to review and implement policies, review all multi-channel routes for data to enter and leave our business, educate the business in what they have to do and the penalties for not doing it. However in the longer-term I think complying with more rigorous regulations will ultimately help companies like ours demonstrate we are a responsible organisation that can be trusted with customer information.

Posted by Julie R on 15 Mar 2017 7:44 PM

Julie I manage a hotel and am responsible for customer data and for credit/debit card information. Data protection insures that the above information is held securely both for paper records and those held on the computer system. GDPR provided a framework to ensure that companies abide by the regulations. For example we check out card machines every 3 months to keep within the compliance regulations. Its strengths are that the systems are regularly tested, but it weakness is that just because you have tested it on a Monday does not mean it is totally secure on Tuesday.

Posted by Grace B on 15 Mar 2017 8:02 PM

Grace, a business owner in the hospitality sector. Data protection is one of my many roles as a business owner. It involves the responsibility for customers personal details both in paper and digital formats and can be a somewhat daunting and time-consuming experience to manage alongside other responsibilities. I am aware of the GDPR through regular updates from business newletters and my own personal research. I can see the benefits of the GDPR in further unifying expectations and consequences across all participating parties, however for small companies it becomes another added source of concern that requires time to understand and implement, all of which comes at a cost.

Posted by Anja K on 15 Mar 2017 8:11 PM

- 1. Anja 2. Analytical Lead 3. Government 4. Handling some FOIs, Governing Official Statistics schedule and content, making data accessible to the public

Any personal information that we hold either internally or on those we regulate, those who approach us or any others that provide information to us for business or employment purposes. Tracking of any information that might identify individuals or businesses.

- I am aware of the regulation for several reasons. In part, it is an aspect of my role that I am up to date with data regulation. Im am not the lead on this but many of my decisions are underpinned by similar legislation. Moreover, I am due to move to a new role where data handling comes with a greater degree of risk, and will need to be well informed of the changes. Also, I have a keen interest in the public sharing of data, like many I feel the benefits of some sharing, however I have concerns over how easily data is sold and shared. My understanding is highlighted as a regular user of research tools that rely on such data being accessible.
- The move towards greater individual data security is essential, overdue and will not be enough at this stage. It is a step in the right direction.

Posted by Sue C on 15 Mar 2017 11:43 PM

Sue, I am employed by county court as admin clerk, responsible to general public to secure personal details re small claims. I am aware of GDPR and believe its a good thing to protect personal details.

Posted by Ian T on 16 Mar 2017 8:26 AM

My name is Ian and I am a director of two children's nurseries. I am responsible for ensuring that our data is kept secure and joined the ICO last year.

When I think of data protection, I think of paper, photographs, data sticks and hard drives. This is where most of our data is stored.

I am aware of the General Data Protection Regulation but don't know much about it yet. I have read about it online.

From the little I know, it appears to be a regulation to control the personal data of people within the EU by companies that work within and outwith the EU. It looks like it will further enhance the current regulations that are in place.

A5.3.2 Day 2: Subject Access Requests & Right to Erasure

Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed; access to their personal data; and other supplementary information. (Subject Access Requests)

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, e.g. where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; when the individual withdraws consent; or when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing. (ICO)

- How does the situation in respect of data access and erasure under the GDPR compare with the current situation (DPA)?
- How important are the rights to data access and erasure for enabling consumer confidence relative to other sources of consumer confidence (such as a track record of data security, brand reputation, any associated risks)?
- What proportion of your customers/data subjects do you expect to exercise the right: (a) To access their data? (b) To erase their data?
- Do you envisage the right of access to data to increase the willingness of individuals to provide personal data to your organisation?
- Do you envisage the right to erasure to increase the willingness of individuals to test services that require the disclosure of personal information? Will this increase the conversion rate?

Posted by Anna T on 16 Mar 2017 7:12 AM

1. Currently within the education sector all information is kept for archival purposes and never erased 2. Rights to current and archival data access are important for continuously freedom of information requests about the institution's history 3. Any data that is kept against individual records is in the first instance assessed to ensure that it is not in breach of confidentiality agreements. Upon assessment, all data is then kept and accessed by the data team at ease. 4. Yes 5. As my institution is currently developing a new record keeping system, We are in the process of testing how user friendly our information can be ie whether we will provide rights to our customers to amend information (erasure). Whether this will increase the willingness of customers i am unsure.

Posted by Ian T on 16 Mar 2017 8:43 AM

I believe that the rights of people to access end erase their data is enhanced with GRPR. The importance of the rights to data access vary depending on the business you are in. We don't expect many of our parents will ask to access their data or erase their data but, potentially, as the knowledge of GDPR is made more common, we may get these requests I don't envisage any difference in the willingness of individuals to provide personal data. I think the right to erasure will increase the willingness of individuals to test the services. I am not sure how this will affect the conversion rate

Posted by Judith B on 16 Mar 2017 9:04 AM

Currently the individual doesn't have the right to be forgotten. Within my remit I have only had one occasion when an individual has asked for something to be erased and I was unable to comply but did notate our record with the inidividuals request. I think this one might prove to be a talking point when individuals become aware that they have this new right. Perhaps because of the nature of my organisation this won't be a major issue but I can see that it might increase workload while each request is discussed. Only based on historical data I can't see that there will be a huge impact on my team.

As for individuals providing personal data, again within my remit this is a necessity but only from the perspective of recording clinical information. My question on all of this is public awareness. Will the public really be fully aware of the new rules and their rights? How many people in the public domain know about dpa and their rights to request information? This is truly an unknown and until it comes in to place and we can assess the impact then I don't know how the public will react. Are we worrying about something that might not happen or are we being naive?

Posted by Rhiannon R on 17 Mar 2017 4:18 PM

Hi Judith,

What might the implications be if people were more aware of GDPR? How do you envisage they might react, and what impact might that have on your organisation?

Thanks,

Rhiannon

Posted by Barbara D on 16 Mar 2017 2:09 PM

1) The right to be forgotten will be a new addition to the legal framework. Data access provisions seem to be roughly the same.
2) I think they are crucial in terms of generating confidence with regards to the whole subject of data protection. Direct consumer/user "control" over abuse makes for a healthier system
3) I think the impact on our business will be minimal. I would say 10% (or less) would request either a) or b). The erasing of data is a sensitive issue given that we are a regulated industry and data must be stored for a mandatory length of time. I can see there being some tension between the GDPR and the perceived right of the individual to be forgotten and "compelling reasons" to store data for some time e.g. legislation relating to KYC and AML.
4) The submission of personal data is often seen as an annoyance and is really considered a necessary means to an end i.e. to use a service or purchase a good. I don't think it will increase the willingness to provide data, but it certainly gives those who provide the data greater peace of mind. I don't think any changes should be seen as justifying the collection of more data.
5) The willingness to participate in tests is really a question of relevance to the individual in question. Whilst interest drives the decision, the "right to be forgotten" is another good reason to go ahead. It may sway those who are "undecided" and convince them to take the plunge. If more people participate then the conversion rate should rise. However, I do fundamentally believe that the test itself must be a positive experience in order to close the deal.

Posted by Linda C on 16 Mar 2017 7:03 PM

- I understand access rights under the new regulations to be more stringent and that the 'right to be forgotten' is new under the GDPR
- In my experience customers are more sensitive to the risks of data security than they are to the rights of access or erasure; however if there were to be any security or other breaches, the way we react to access and erasure requests would become critical to protect the company's reputation as a responsible holder of information
- I wouldn't expect very many to exercise their rights at all, and it would probably be in the case where a customer were unhappy about another aspect of doing business with us. Very few customers have ever requested sight of the information we hold for them
- I don't expect customers' willingness or otherwise to provide personal data to my organisation to change as a result of GDPR
- I think as long as customers can see a benefit to them of providing personal information in order to access the service and if it is made explicit that personal information will be deleted on request, then I would expect to see an increase in disclosing information and an increase in conversions

Posted by Olivia J on 16 Mar 2017 7:27 PM

Thanks Linda. why do you think customers may not do so?

Posted by Rhiannon R on 17 Mar 2017 4:24 PM

Linda raises an interesting point, saying "the way we react to access and erasure requests would become critical to protect the company's reputation as a responsible holder of information"...

I'm interested in everyone's thoughts: to what extent would you take a customer's access/erasure request as a warning that something is going wrong? Would it feel in any way as if you had lost users' trust? Why/why not?

If you were to feel as if you'd lost users' trust in any way, would that act as an incentive to look into your organisation's data protection/security processes?

I look forward to hearing all of your thoughts on this - thanks everyone!

Rhiannon

Posted by Judith B on 17 Mar 2017 8:57 PM

I would become concerned if I started to see either an increase in requests or a trend for a specific erasure request. I would also say that in dealing with all requests I consider the reputation of my organisation on all occasions. I have also learned that client demand is changing and becoming more complex. In a world where information is available instantly on so many subjects people are demanding more and expecting it.

Posted by Barbara D on 18 Mar 2017 10:49 AM

I would only be concerned if this behaviour was replicated by a significant number of consumers. There will always be cases where people will ask for access/erasure - but these may be "outliers". I

think the trust element is a function of a number of different factors, one of which is treatment of data.

Posted by Anja K on 18 Mar 2017 3:59 PM

Requests like this, if sporadic probably wouldn't cause alarm due to the content of information we work with. If there were emerging patterns, we would conduct further analysis or surveys to identify the root of the problem.

Posted by Gill K on 16 Mar 2017 7:30 PM

The right to erase is too broad a brush. People who have been convicted, or cause in indiscretions, particularly those in public office should not be allowed the enhanced 'right to be forgotten' under the GDPR. Difficult to say how important the 'right to be forgotten' can be. It will depend o. Each set of circumstances. Unlikely any of our clients would want to erase any of our data, but it is possible. Greater disclosure will cause people to be less likely to give personal data. Unlikely, the information will be 'out there' for however a limited period.

Posted by Rhiannon R on 17 Mar 2017 4:15 PM

Hi Gill,

You make an interesting point about the 'right to erasure' as being a broad brush.

What other groups of people / organisations do you think shouldn't be granted this right? Is it black/white - why or why not?

Thanks,

Rhiannon

Posted by Gill K on 17 Mar 2017 10:48 PM

I would questions if anyone or any organisations should not be granted 'right to erasure'. Everyone should have access, but who decides if something should be erased is the problem.

Posted by Grace B on 16 Mar 2017 7:32 PM

Data access rights will remain fairly similar though the erasure will be a new introduction. I believe data security is not at the forefront of customers minds until there is reports of a data breach (which considerably reduces consumer confidence) whereas brand reputation is more readily apparent and thus more important, however the new guidelines should help to give customers piece of mind through their transparency and increase confidence overall.

I have yet to have a customer question any data held and I don't envisage this changing unless GDPR gets enough coverage from the media to raise awareness of their rights in which case possibly 10% at most may choose to access or erase.

I don't imagine the right of access nor erasure will change individuals willingness to provide personal data to my organisation as it is within their interest to do so in order to receive products/services though we are able to be somewhat more lenient on what data they do supply so they are able to

provide what they are comfortable with us storing. I wouldn't know how this could effect the conversion rate.

Posted by Anja K on 16 Mar 2017 8:34 PM

- Personal data currently has to be kept on file for 5 year in circumstances relevant to my work. After five years it must be deleted.
- Rights to erasure sounds like something we should have had for a long while regarding consumer confidence. I'm not sure how this applies to data that might support criminal behaviour identification though, I suspect where data is evidence the consumer might be more likely to request erasure. As we live with constant security uncertainty, erasure is an attractive prospect from a consumer perspective and hands back some control. It will probably be as effective as regulation, in that a company with a licence to operate is more trusted than one that isn't.
- I think that there will be fairly low uptake given today's data-sharing environment, but the option will prove a valuable attraction for consumers. In time, I think it will be more common to request erasure. I'm less sure about access as the proportion of people benefiting from this is likely to be quite small and due to fairly niche issues.
- Probably, yes. But as part of a broader theme of confidence in information sharing, rather than specific to our organisation.
- Possibly, this is a real issue in our area for testing products. I imagine it will make people more willing to test some of our processes on home computers etc.

Posted by Julie R on 16 Mar 2017 9:56 PM

We keep all records for 5yrs plus the current year for tax purposes, but this includes all customer booking details. After we have kept the details required for tax they are shredded on site and composted. It would be fairly easy to confirm which details we hold for individual customers and to erase their data if requested. I do not expect anyone to request acces to their data, nor to ask for it to be erased. I do not envisage the right of access or erasure of data will have any imperceptible to customers using our services.

Posted by Sue C on 18 Mar 2017 10:07 AM

Currently data protection is in line with the human rights act. I believe there will be minor changes. Very important for consumers to be able to access data held on them although the general public will be more aware because of the change and will probably increase the number of consumers that wish data to be erased especially when it is years old as in old addresses etc. hard to predict a percentage. I think consumers will have more confidence in providing data knowing they can apply for hreater protection We take data loss very seriously at work.

Posted by Nigel B on 18 Mar 2017 6:24 PM

It improves individual access to data and gives the right to erase. It's more in tune with social media current issues.

I hope it improves access and make people more comfortable with whoever is holding their data. It stop use of DP as a standard deterrent answer for not being given data.

I do not expect any increase / decrease in access from my clients.

In some circumstances I would envisage an increase in erasure of data after the completion of a behavioural project where clients feel holding onto their individual data may be too tempting for management to resist using it for some other reason to the individuals detriment.

There may be a increase in conversion rates due to the nature of our work with our clients in behavioural team building.

A5.3.3 Day 3: Subject Access Requests & Right to Erasure (2)

Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed; access to their personal data; and other supplementary information. (Subject Access Requests)

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, e.g. where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; when the individual withdraws consent; or when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing. (ICO)

1) How big a problem is inconsistent/out of date personal data?
2) Will the right to data access and erasure improve the consistency of data?
3) What is the value of more consistent data to your organisation?
4) Have you taken any steps to enable access to / erasure of the personal data you hold in anticipation of GDPR? What did that cost?
5) Do you envisage the right of data access to lead to changes in your organisation's data sharing practices?

Posted by Anna T on 17 Mar 2017 7:09 AM

1. The problem of accountability is severe especially when it comes to an audit 2. Providing individuals more control over their data may make it more consistent 3. The value of consistent data is especially important for accurate reporting 4. We are currently working on creating a new information management system and the cost of restructuring is very high 5. No, as there are principles that will overrule info access, particularly in relation to student data reporting

Posted by Barbara D on 17 Mar 2017 9:52 AM

1) The problem is huge - both in B2C and B2B. Especially in B2B the lack of consistent up to date data is a major obstacle to communication with suppliers and the implementation of early payment programmes - some buyers just don't know howto contact suppliers in a timely manner.
2) The fact that a right is given does not mean it will be exercised. I can only see consumers/users using this right were they to be in "conflict" or have specific issues with the entity holding the data. To improve consistency there must be some incentive for the consumer/user to amend and erase. Without such an incentive I cannot see consistency improve.

3) Consistent data is important in my organisation as it fulfils part of regulatory requirement. A lot of time and cost is dedicated to having consistent data and reporting this data in a timely fashion.
4) No, we have not taken any steps as yet and have no clear of future costs which will be incurred.
5) No, we have confidentiality requirements which limit any data sharing.

Posted by Linda C on 17 Mar 2017 8:04 PM

1) It's a big problem. With 30%+ of B2B data churning every year, it's impossible to keep personal information up-to-date. We constantly grapple with issues caused by customers having moved roles/left businesses/changed names
2) Assuming enough customers exercise that right then I would expect the consistency of data held to improve
3) Sales and marketing effectiveness, improved customer experience through us knowing and understanding customers better, more accurate financial reporting and insight
4) No, we have not yet taken any steps in anticipation of GDPR. However, we are starting to look at mass archiving and deletion of old data (dormant accounts, web registrations etc)
5) I don't expect the right of data access to lead to changes in our data sharing policies - which are already tight - but I do anticipate a thorough review of current compliance to policy

Posted by Judith B on 17 Mar 2017 9:04 PM

there isn't an issue with out of date/inconsistent personal data within my organisation. The nature of the service would not generate this kind of issue. Just yesterday I had a lengthy debate on this subject with the person who is dealing with the roll out of GDPR for our organisation. A mini brainstorming session to look at what kind of scenarios would occur that a client would ask for something to be erased. Given the nature of our line of work it was agreed that each case will have to be decided on individually and also we might need to seek legal advice also. I work in the Emergency health sector and personal data has only once caused a client to ask for something to be erased. I might be naive in thinking that this won't be a huge issue for us as it hasn't been so far!

Posted by Julie R on 17 Mar 2017 9:21 PM

We don't really keep data too long. It will only be inconsistent if there is a change of address or phone numbers. If the data us input incorrectly and the person asks for access the data will be updated, or erased as necessary. The value is personal marketing and future bookings and sales All customers complete a form with tick boxes if they do not want their info stored, access to info is reasonably straight forward. Paper details are also easy although time consuming to collect. I think we currently do all that we can to provide access so no further changes will be required

Posted by Gill K on 17 Mar 2017 10:45 PM

1. A very large problem. Trying getting errors in your meducal records changed. It is practically impossible. 2. Unlikely, one has to take into account human errors, cross wires, just bad inputting, or people putting in recotds what thry think, raer than what someone actually said. 3. More consistent data would ensure correct information on client's files, which could elimate misunderstandings and unforeseen consequences. 4. Access is already available at the client's request. Most clients do not ask for avpccess, so erasure has not yet become an issue or a cost. 5. No, for clients, see above.

Posted by Anja K on 18 Mar 2017 1:22 AM

1. Inconsistent/out of date data is a big problem because it does not tell the truth. 2. Yes. 3. It provides better evidence for enforcement. 4. Not yet, but we intend to. 5. Yes, we will delete data as requested.

Posted by Ian T on 18 Mar 2017 9:54 AM

1) I would imagine that there is a huge problem with out of date data. With personal circumstances changing all the time, there is no way that the companies who hold the information will be able to keep it up to date.
2) This should improve the consistency of the data bit it depends on how many individuals exercise their right to have their data removed.
3) Consistent data is important to our organisation and we send out an annual request to customers to update their details. Not all do it but it does prompt the ones have changed to let us know.
4) We have not taken any steps sp far as it would not be a big problem for us to erase the data being a relatively small company.
5) I don't expect that this will lead to changes in our practices as we are already very secure

Posted by Sue C on 18 Mar 2017 10:15 AM

I would say a big problem when it comes to receiving notifications of important info like a parking fine which can quickly escalate into a bigger problem if for example sent to an old address. I believe it will improve it greatly. Less time wasted correctinv out of datd data. I have not taken steps but am interested in doing so. Definitely will be changes makes sense to do so to improve relations with consumers.

Posted by Nigel B on 18 Mar 2017 6:30 PM

1) We tend to only hold data for the length of a project or it is reviewed / updated annually.
2) In our case no.
3) More accurate results and hopefully better quality of individual answers
4) We have not had to change our procedures yet and have not incurred any costs. Since we review / erase annually anyway it is not expected to increase our costs
5) It may added some further controls to monitoring access and therefore some changes to processes.

A5.3.4 Day 4: Fines

Under the GDPR, supervisory authorities are empowered to impose significant administrative fines on data controllers and data processors. Maximum administrative fines of up to €20,000,000 or (in the case of undertakings) 4% of global turnover can be imposed for infringements of the basic principles for processing, including conditions for infringements of consent (Articles 5, 6, 7 and 9); data subjects' rights (Articles 12-22); the rules on international transfers (Articles 44-49) and others.

1) Do you envisage that an increase in the severity of fines for failing to protect consumer data would lead to your organisation taking data protection more seriously? Why or why not?

2) Have you taken / do you expect to take any additional security measure in response to the increase in maximum fines for data breaches?
3) Do you envisage that an increase in the severity of fines for failing to protect consumer data would increase the willingness of individuals to provide personal data to your organisation? Why or why not?
4) How, if at all, will this benefit your organisation?

Posted by Anna T on 18 Mar 2017 7:28 AM

1. Yes, although public sector organisations are already governed by strict pressures 2. Yes we are working to provide more transparency for our data 3. No, as changes to institutional pressures are noticed more by staff than by consumers 4. I suppose the overall benefit would be that there will be a move to more accountable practise.

Posted by Ian T on 18 Mar 2017 10:18 AM

1) It certainly highlights the importance of protecting consumer data but our processes are already very secure and I don't think that we would change them.
2) I do not expect to take any additional security measures in response to the increase in fines.
3) Yes. I think that individuals would be more willing to provide personal data if they thought that it would be stored more securely. The instances of data breaches (Yahoo, TalkTalk etc.) in recent years has highlighted the security (or lack of) of personal data.
4) I do not see it benefiting our organisation as we already have complete data records of our customers and do not have any problems in obtaining these.

Posted by Barbara D on 18 Mar 2017 10:36 AM

1) Not in our case, as I have mentioned elsewhere our processes are already very robust due to stringent regulatory requirements. The severity of the fine will undoubtedly deter bad practice and lead to organisations in general improving practice and processes, although cost is a factor here and smaller companies may be adversely impacted. However another essential consideration is how effectively the supervisory function is exercised. If the fines are high and supervision lax then the regulations will not be taken as seriously.
2) No, our treatment of data already conforms to stringent controls from the regulatory authority which supervises our sector. Our security measures are fit for purpose for the foreseeable future.
3) The increased severity of fines will act more on the organisations than on consumers. Data exchange is essential for nigh on every transaction these days and consumers grin and bear it regardless of the level of protections they are afforded. Consumers assume that the organisations they are dealing with - especially the larger ones - fully comply with all regulations.
4) We already function in a sector where regulation is tight and the levels of checks and controls companies must exercise are numerous. This will add another layer of compliance companies like ours must abide by - and probably a number of provisions will overlap. I am not arguing that there should be no control, or less control. There are benefits to consumers and society at large, but from a company stand point it is another bureaucratic hurdle and potentially more cost.

Posted by Sue C on 18 Mar 2017 10:59 AM

Our organisation takes it seriously already. Expect to take more security we are always looking at ways to prevent data loss. I dont think willingness will improve, I believe unless you are in the know would you care what the fines are to others. In some circumstances they may not have a choice if providing info is of benefit to the individual. Little or no benefit to any party. I believe Fines are a 'money making' exercise with little of the finance going towards improvement of systems.

Posted by Gill K on 18 Mar 2017 12:53 PM

1. No, it is taken seriously now. 2. No, we try to ensure we comply fully now. 3. No, individuals will never or rarely ever want to give their personal details. 4. Does not benefir our organisation either way.

Posted by Judith B on 18 Mar 2017 3:11 PM

1. My organisation currently take data protection very seriously. We aren't perfect and the introduction and roll out of GDPR will raise awareness and hopefully increase behaviours and awareness of our people. 2. We continue to strengthen security using new technologies. For instance secure email rather than handing over disk with call recordings on. New procedures and practices will also help increase security. 3. No I don't see a change in what personal data we obtain. As an emergency service we only take relevant information which can't really be avoided and rarely is there reluctance with provision. 4. I don't perceive any increase in benefits

Posted by Anja K on 18 Mar 2017 3:55 PM

1) Possibly, although as a government organisation credibility is key to our work regardless of financial penalty. Falling foul of regulations is a huge risk.
2) No, although existing training will always be updated to reflect changes. It might encourage individuals to take policies seriously.
3) I believe that people who share their data with us are confident in handling processes, I'm not sure we will see much of a change as a result of these changes however for overall consumer perspective might help build confidence in sharing information as part of daily life.
4) Probably as a benefit in changes to information sharing attitudes among the public, we might see people more willing to approach us and thus improve regulation. It is more likely to be secondary benefit than an immediate and directly related change. As operators we regulate improve, it is likely that our reputation will do as a result.

Posted by Nigel B on 18 Mar 2017 6:42 PM

1) The increase in cost of fines would effect us. If we felt we were being targeted or individuals were trying to make money from challenging us we would have top take steps to mitigate these costs.
2) We are reviewing this situation. We may increase levels of encryption, password change frequency and use of two stage or one use password strategies. Tighter restrictions on USB and mobile device access may be required to protect data sources during transit.
3) I do not think the severity of fines is of interest to individuals only government departments to be seen to act. The more valuable the data the more likely that someone will want it and pay a third party to obtain it. Severity of fines will not change this in any way but may make poor quality companies spend more on their system to secure their data more.

4) No additional benefit to our organisation but will be additional level of monitoring and control at addition cost.

Posted by Julie R on 18 Mar 2017 7:47 PM

We already have procedures in place for data protection which are quite robust, however the severity of the fines will concentrate the mind to ensure that the procedures are followed to the letter. Our current procedures should be good enough. I think customers are becoming more savey with what information they provide and will leave gaps if they don't want you to know or they believe it is not necessary. I cannot see how this would benefit our organisation as I think we are doing everything at the moment to comply with with they new regulations

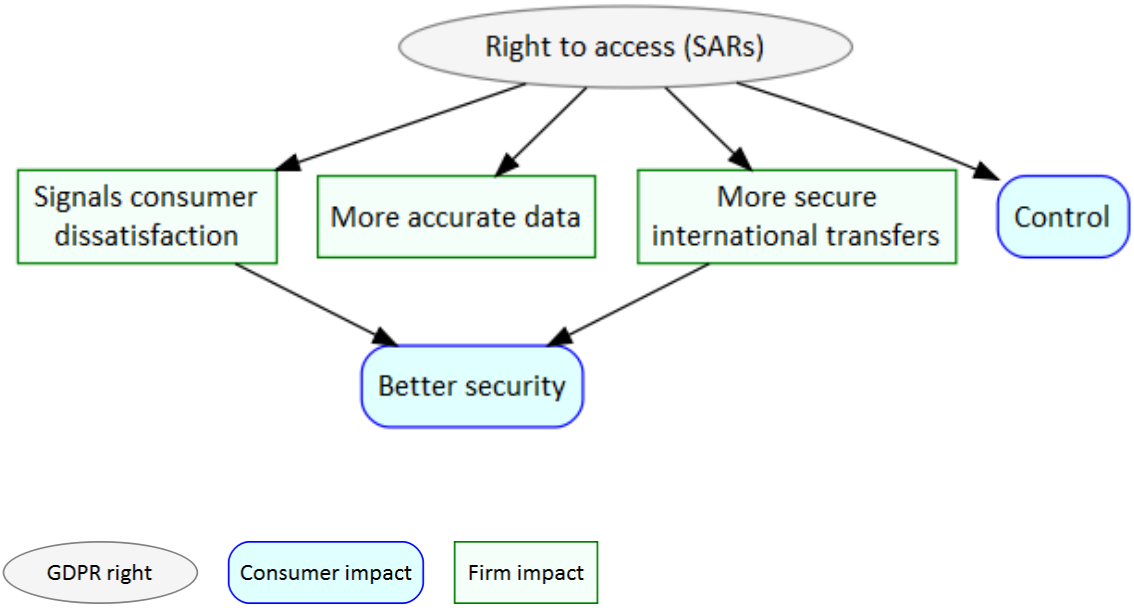
Posted by Linda C on 18 Mar 2017 7:55 PM

1) No, the company already takes its responsibilities very seriously and the right people are aware of the role they need to play. I do think the increase in severity of fines will raise the profile of data protection in the organisation.
2) No, we have not taken additional measures and do not expect to
3) No, I believe our customers already have a high level of trust in us and therefore would not expect anything to change on the basis of a significant increase in penalties for data breaches. I believe customer loyalty is influenced by the company's reputation and performance across the whole customer journey, so if we consistently failed to secure customer data it would have dire consequences
4) If it ended up being a positive differentiator then of course it could have commercial benefits in terms of customer loyalty, increased retention and additional sales. But that's only on the assumption all the competition fail to comply with the new legislation. Otherwise,no additional benefit as we already take the issue seriously

Annex 6 Original mapping of potential benefits from GDPR rights

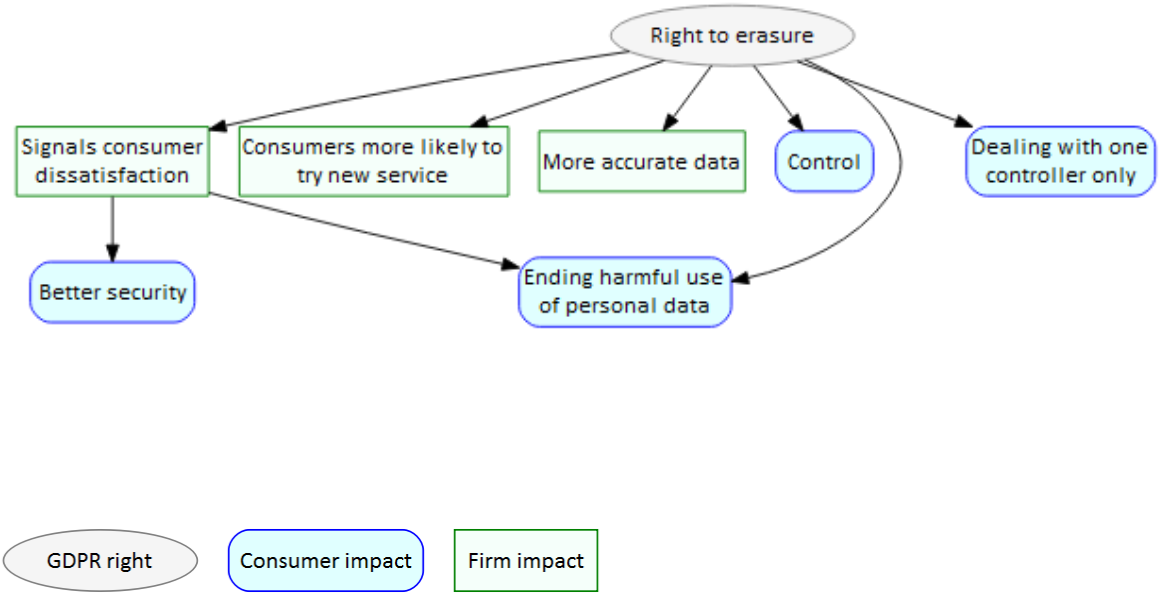
This annex presents the original mappings used to conceptualise potential benefits arising from the rights to access, erasure and data portability. These have been used to structure the thinking for this report. The main body contains the mappings of rights that have actually been tested in the data professionals' survey.

Figure 80 Benefits arising from the right of access: original



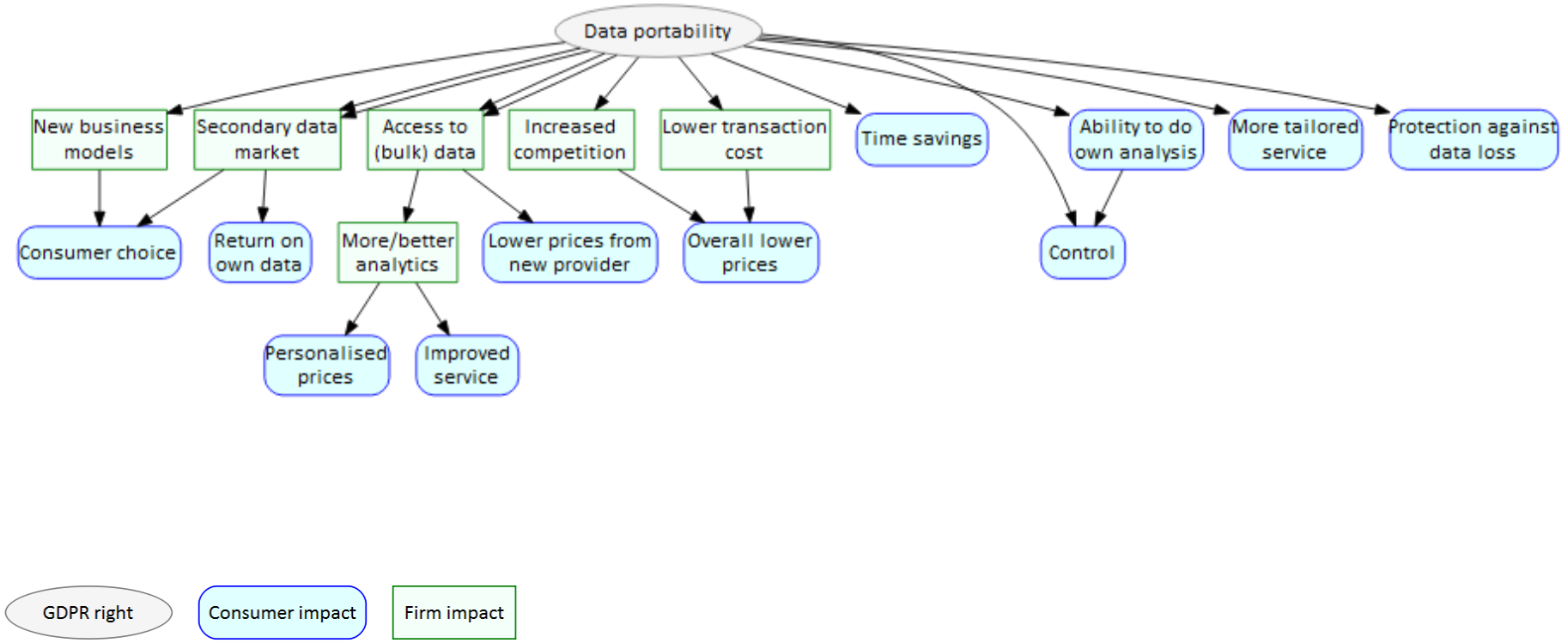
Source: LE

Figure 81 Benefits arising from the right to erasure: original



Source: LE

Figure 82 Benefits arising from the right to data portability: original



Source: LE

LE London Economics

Somerset House, New Wing, Strand,
London, WC2R 1LA, United Kingdom
info@londoneconomics.co.uk
londoneconomics.co.uk
@LondonEconomics
+44 (0)20 3701 7700