dataIQ

Industry Research

Ready or Not?

Preparing for the introduction of a new Data Protection Regulation

November 2012

Prepared by:

DQM Group™
CONFIDENCE IN DATA

Contents

Introduction

Dramatic changes may soon be necessary to the way personal information is captured, processed, analysed and managed. If a proposed new law is passed, within two years permission may be required for every aspect of data management - from processing through to targeting and even profiling.

In January 2012, the European Commission published a new Data Protection Regulation. Its intention was to improve consumer rights, recognize the expanded domain in which data is generated and used and reflect new security challenges and technological opportunities. It was claimed at the time that the measures could even save billions of Euros in business costs.

Since these proposals were tabled, businesses have examined how they would impact on existing processes and technologies, leading to concerns about costs, constraints and compliance. For UK businesses especially, the demand to level up to standards imposed (although not always followed) in Germany and Spain would be onerous.

DQM Group commissioned exclusive research among UK marketers to identify where the pain points and likely challenges sit within these proposals. This whitepaper examines the shifts in core data protection laws being proposed, their likely impact on marketing and the findings of the survey into how prepared UK industry is to respond.

Executive Summary

Personal data could be redefined to include data elements, such as IP address or mailing address, which are not currently described as personal information and do not therefore fall under the existing data protection laws. Clarity about this definition has been widely called for.

Consent would also be redefined to become specific and explicit, rather than implied. Half of companies expect this to mean an opt-in mechanism and a need for better permissions management. While 85 per cent of companies already gain consent, only 55 per cent keep clear records of when and where this happens. If consent continued on an opt-out basis, its impact would be largely manageable, according to marketers surveyed by DQM Group. More difficult would be extending opt-outs to profiling, although this is seen as preferable to having to gain an opt-in.

Privacy policies would need to provide much more detailed information and be easier to understand - the DQM Group survey found that a small minority are confident they already offer this. There are significant gaps in the information which is being provided, however, with only six out of ten explaining how data can be accessed, changed or deleted and just one-fifth explaining how long they will retain data for.

Requests to see and correct data are expected to increase if the current charge for this is removed. This is likely to be challenging for the half of companies which do not have clear, written processes in place to handle these requests. The Right to be Forgotten has gathered most attention in the proposals with businesses concerned about how this right could be enacted across an eco-system of linked, distributed information systems. Only one quarter of companies told DQM Group that they had an annual data deletion process while exactly the same number never delete data.

Data portability is another key right being proposed that would be difficult for many companies to support. Given the enhancement and transformation which personal information undergoes, there is a fear that data could not be easily released in this way - only one quarter of marketers say they understand the need and would help.

Although data protection processes are widely understood, only 54 per cent have embedded privacy controls into system lifecycles. Independent auditing is used by just one third of companies and even fewer have completed a Data Protection Impact Assessment, which could become mandatory under the proposals. Just one fifth measure privacy controls as a performance indicator.

Data breaches have gained a lot of media coverage in recent years which has helped to drive up awareness of the need to protect personal information. This is reflected in the relatively high confidence levels around data security measures found in the survey, but the need to notify the regulator of a breach within 24 hours would still be hard to carry out. There is also a risk of a resource gap around the employment of independent data protection officers, should this requirement be imposed by the new regulation.

Scope and Impact of the Proposals

1. Definition of a data subject

Article 4 of the proposed regulation sets out the following definitions:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information relating to a data subject;

This would appear to have two important consequences:

- IP addresses as well as locational data could become classified as personal data (although this may depend on context);
- A physical mailing address (without an attached name, but where the occupant's identity might be known separately) could be considered personal data.

The vast majority of companies who commented on the proposals to the Ministry of Justice felt strongly that there is a need for clarity on this definition of personal data.

Respondents from the information technology industry argued that an internet protocol (IP) address does not necessarily identify a person, but rather a device that uses the IP protocol.

The importance of this definition is in how it might bring categories of data under the data protection legislation which are not currently captured according to its requirements. So any digital marketing or mobile marketing activity, for example, would need to be capable of levelling up to the data protection standards currently applied to personal data within the existing definition.

2. Principles (Article 5)

These have been simplified and reduced, although the net impact on business is probably greater as the existing security and transfer principles have been subsumed into the other principles.

The new emphasis on transparency, the clarification of data minimisation and making the liabilities of controllers and processors a Principle are key points.

Crucially, consent will have to be "specific" and "explicit", not implied.

In responses to the Ministry of Justice, over half of respondents felt that the use of the term explicit in the context of consent would require data controllers to provide data subjects with an opt-in to the processing of their personal data, where this processing was based on the consent of the data subject.

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

In addition, Article 7 sets out the following as one of the conditions for consent:

"The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes."

This would require strong permission management by any company capturing personal data in order to demonstrate when and where they gained consent for its usage.

In the DQM Data Protection Survey, there is evidence that consent is being obtained fairly and transparently, albeit under existing opt-out standards (see Chart One). However, permission management is weaker and represents an important challenge for data managers.

Chart 1: The Principles

3. Lawfulness of Processing (Article 6)

"1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes..."

The importance of data subjects' rights in controlling usage of their personal information needs to be balanced with the legitimate reasons which data controllers have in processing data in order to run their business and deliver products and services.

The core concern with this proposal is around the nature of the consent which will be required for any data processing. In the course of contractual engagements, there are unlikely to be any problems in ensuring appropriate consent.

However, many services are currently delivered with no direct contract, eg, provision of web site content, search, social networks, etc. In these circumstances, data processing is essential. Consumers have shown relatively little concern that their privacy is being violated or their rights abused, providing they see an appropriate value exchange.

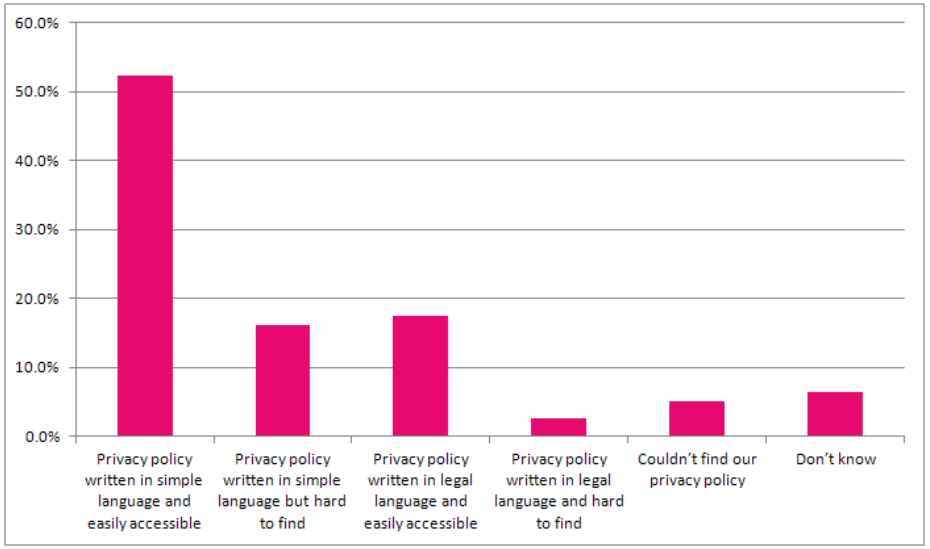
Active consent in the form of an opt-in is regularly shown to reduce the number of permissioned data records by around 400 per cent. This would prove financially disastrous for most commercial organisations. Consent to data processing would therefore need to continue to be on the basis of opt-out, not opt-in if current data management processes are to be maintained.

4. Transparent information & communication (Article 11)

- Data protection policies will become considerably more evident and transparent to the consumer, much as the ePrivacy Directive has placed cookies notices right at the start of an interaction. Just as with the change to cookies, marketers may be concerned about the impact this could have on the customer journey.

At the very least, privacy policies will need to become clearer and more accessible. Chart Two suggests that half of organisations will not find this difficult, but that there is some way to go for the rest. Just over one third of marketers (36.6 per cent) review their privacy policy on an annual basis, but nearly the same proportion (32.8 per cent) did not know how often such reviews took place. Half of marketers would find it difficult to tailor their privacy policies to the needs of different audiences.

Chart Two: Clarity and Accessibility of Privacy Policies



5. Rights of the data subject (Article 12)

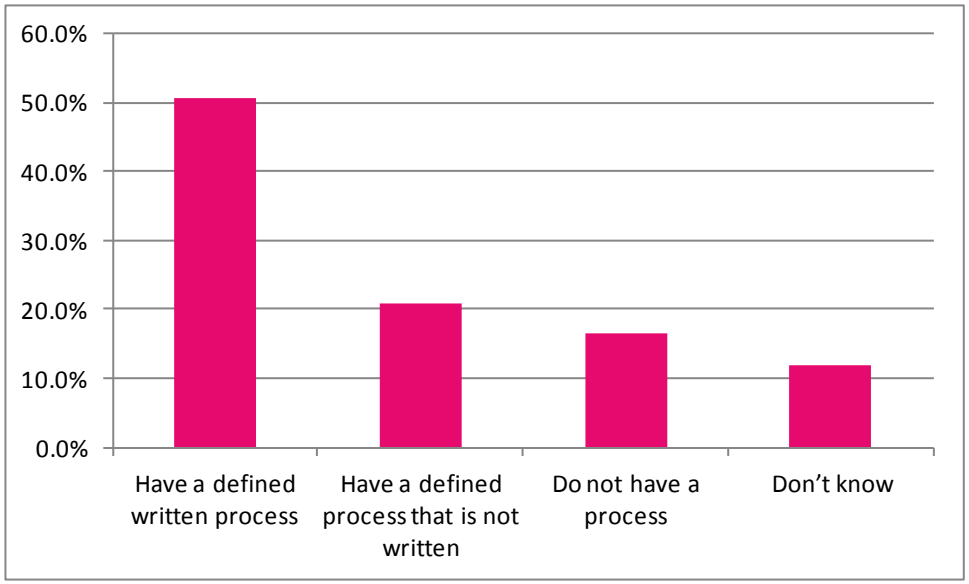
- Data subjects would gain the ability to transfer personal data held on them by controllers, as well as requesting access, changes or deletion. The legislation would expect controllers to facilitate these requests within a month, but longer periods may be possible with good reason. Controllers will have to tell the data subject when changes are complete, unless this is disproportionate.

These requests may not be charged for (unlike the current £10 fee for Subject Access Requests) unless the controller can show that they are manifestly excessive and/or repetitive. In submissions to the MoJ, there was a clear contradiction between two sides of this argument.

Overwhelmingly, rights groups and members of the public agreed with the proposed change to make subject access requests free of charge. However, businesses and other organisations did not welcome the removal of the ability to charge a fee. They have predicted an increase in the volume of subject access requests they receive if the fee is abolished, which would have detrimental effects on resource capabilities and budgets.

Despite the existence of SARs as a consumer right under the current Data Protection Directive, only half of organisations have a defined and written process for handling them. Although a further one fifth do have a defined process, it is not written down (see Chart Three). Three quarters (73.8 per cent) of companies are able to respond to a SAR within 20 working days of receipt.

Chart Three: Managing Subject Access Requests (SARs)

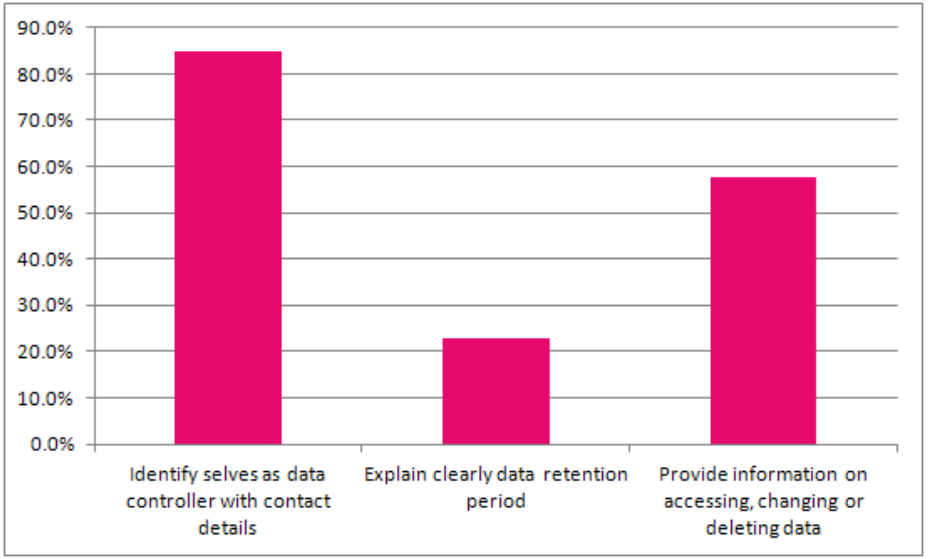


6. Providing information to the data subject (14 & 15)

- Data collection notices will have to be tailored for each situation because of the need for transparency and clarity about the purpose, retention period, further recipients, transfer destinations and data subject's rights in each case.

Subjects would also have to be told about the source of data used in marketing, where this has been collected by a third party, which would be challenging in the case of merged data sets. This information will also have to be made available to data subjects on request at any future point.

Chart Four: Information in Data Capture Notices



According to the DQM Group survey, 84.7 per cent of companies already identify themselves as the data controller, while around 60 per cent explain about access, correction and retention of data. That is a considerable gap that would need to be closed, but not as great as that around explaining the data retention policy, which barely one quarter currently provide information about (see Chart Four).

The majority of marketers (57.7 per cent) currently make no reference to the Information Commissioner's Office during data collection. One quarter do make data subjects aware that they can lodge a complaint with the ICO and provide contact details.

Extending the amount of information provided in privacy notices would significantly challenge the majority of organisations, especially listing future recipients of data, overseas transfers, and the potential consequences of failing to consent to data processing (see Chart Five).

Companies that tell individuals the identity of any future recipients of their data are currently outweighed by those which do not do this (34 v 25.8 per cent). Nearly one quarter (23.3 per cent) say this would be impossible for them to do.

Notification that data may be transferred overseas - and what level of data protection applies in destination countries - is very limited. Just 12.6 per cent do this, with a further 13 per cent mentioning data transfers but providing no details of how it will be protected.

Chart Five: Notification of Rights

Surprisingly, more than half (53 per cent) claim not to transfer data overseas. With current levels of outsourcing and growing use of the cloud for data storage, this level will certainly fall, assuming it is accurate - it is possible that many marketers are unaware of where data is being held.

Just over one third of companies do not tell individuals whether providing personal information is obligatory or voluntary, with information on the consequences if they do not provide this data.

7. Right to be Forgotten and to Erasure of Data (17)

1.The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data.

- Data subjects already possess the right to have data corrected and data controllers are required to limit the data they capture and retain it only for an appropriate period. Providing a thoroughgoing right of erasure and abstention from further dissemination places a disproportionate burden on the data controller and may conflict with data retention requirements imposed by other regulations.

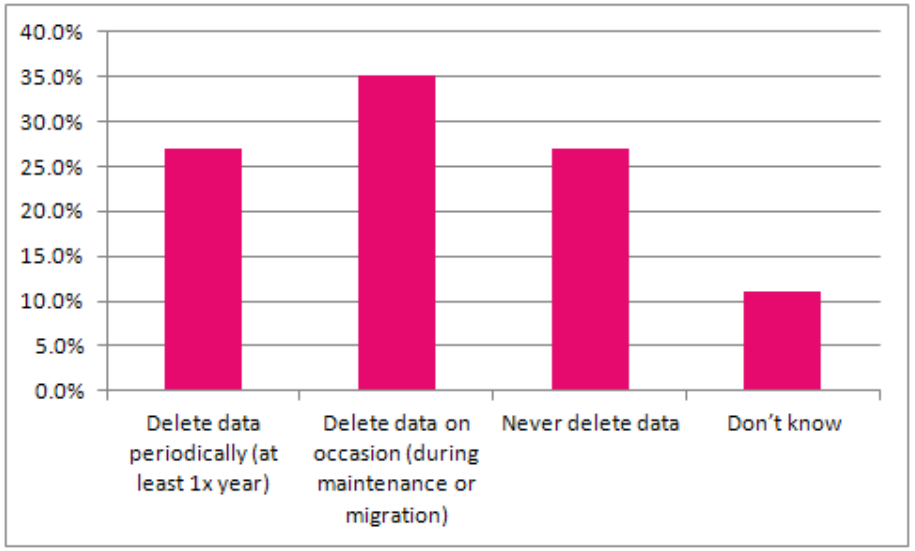
Businesses need to apply a range of processes to personal information, such as reporting, financial and risk management, customer management, etc. Each of these can lead to data being replicated in systems. Desirable and effective business activities may also require the duplication of personal information, such as when an individual applies for a new product, completes an application form which is then passed to a third party for fulfilment of the order. Retrospective deletion of data could prove difficult, depending on the duration of the period over which the right to be forgotten could be exercised.

Equally, the introduction of new generations of information technology will tend to duplicate data. Online data systems and services, such as social networks, also proliferate data at considerable speed. Personal information is unlikely to be limited to a single record.

Simple deletion requests should not present a problem for any commercial or not-for-profit organisation where there is no over-riding legitimate interest in retaining that data, such as to meet other regulatory requirements for data retention or to prevent fraud.

A significant concern about the extension of the right to be forgotten relates to deliberate attempts to remove information from a

Chart Six: Data Retention and Deletion Policies



company's systems in order that a new, fraudulent relationship can be attempted.

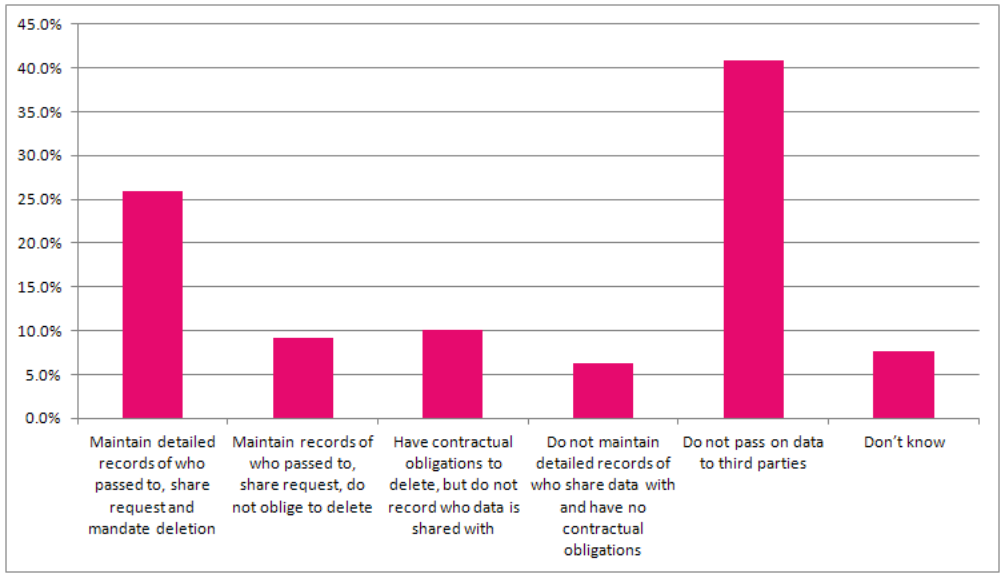
As a result, this proposal would impose an obligation which would be nearly impossible to comply with. This proposal would lead to a significant increase in administrative burden, higher costs, and a potential reduction in corporate revenues. Flagging records which are subject to a Right to be Forgotten request would be more practicable and in line with existing suppression routines.

Data retention and deletion policies are far from being commonplace (see Chart Six). The consensus from the majority of respondents to the MoJ was that the Right to be Forgotten places unrealistic expectations on data controllers, not only to erase all the personal data that they hold on data subjects, but also, where that data has been made public and replicated online, to try to secure its deletion by third parties. MoJ respondents also touched on the financial impact that the 'right to be forgotten' could have on businesses, in particular the cost of changing their business processes to implement the new requirements, which some businesses have estimated at up to £100,000.

The DQM Group survey discovered that sharing Right to be Forgotten requests with third parties would present a major challenge. As Chart Seven identifies, there are major gaps in processes and documentation of data sharing with these external business partners, such as data capture houses, database bureaux, telemarketing agencies and email broadcasters.

Although four out of ten marketers claim never to pass data on to third parties, this may be due to an understanding that the question related to commercial data sharing (ie, where customer data is rented out as a targeting list). Organisations which never make use of any outsourced service provider and therefore never transfer data to a third party tend to be much rarer.

Chart Seven: Sharing Deletion Requests with Third Parties



8. Right to Data Portability (Article 18)

"The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject."

Personal information is the property of the data subject. Equally, extensive data is regularly appended to that personal information by organisations which is commercially confidential and adds significantly to the value of that data asset.

Tests of data portability are already underway in the UK (eg, midata) to empower consumers with better access to their personal information and to open up potential new markets and ways of making decisions, such as choosing new service providers. In these tests, the extent of the data which can be accessed and transferred is in the process of being evaluated with clear parameters being established.

Opening up access to personal information within a data warehouse presents security issues and it may be operationally difficult to link from a system in Company A to a system in Company B due to different technologies, standards, data models and proprietary software. End-user devices held by the data subject will also become storage points for sensitive personal information which could make them valuable targets for criminals.

Clear parameters would need to be set for the level and volume of data which is to be subject to portability, and also to ensure that the process of transmission does not interfere with ongoing business processes.

Businesses have told the Ministry of Justice that data portability would be very draining on resources and costly, particularly for SMEs, who may be inundated with requests from data subjects to have their personal data made available to them in an agreed format for reuse. Businesses were particularly concerned that Article

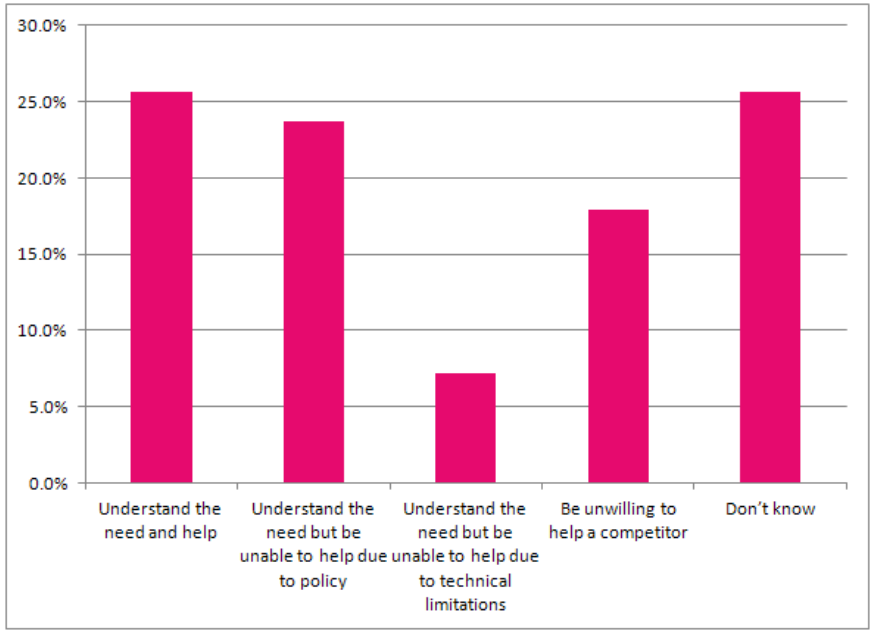


Chart Eight: Data Portability

18 has not left provision for data controllers to protect their trade secrets and intellectual property rights.

This was reflected strongly in the DQM Group survey which found only one quarter of companies likely to be able and willing to transfer data in this way (see Chart Eight). Barriers to transfer exist in the form of either policy or technology at nearly one third of companies, while nearly one fifth see this proposal as anti-competitive.

9. Right to Object to Direct Marketing (Article 19)

Article 19.2: Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing.

- A right to object to the use of data for direct marketing purposes already exists. It is already well understood by consumers and exercised on the basis of an opt-out offered at the point of data capture.

Consumer knowledge and use of this right can be seen in the 41 per cent opt-out rate on the Edited Electoral Register, which allows individuals to withhold permission for their data to be used for direct marketing.

A change in this consent from opt-out to opt-in would have significant commercial impacts, including higher administrative costs and lower revenues. The right to object to direct marketing is only likely to be practicable if it continues to be on the basis of opt-out.

Marketers have expressed a degree of concern about the impact which extending the right to object might have. As Chart Nine shows, one third believe there would be severe or significant impacts, although a similar number expect the impact to be manageable.

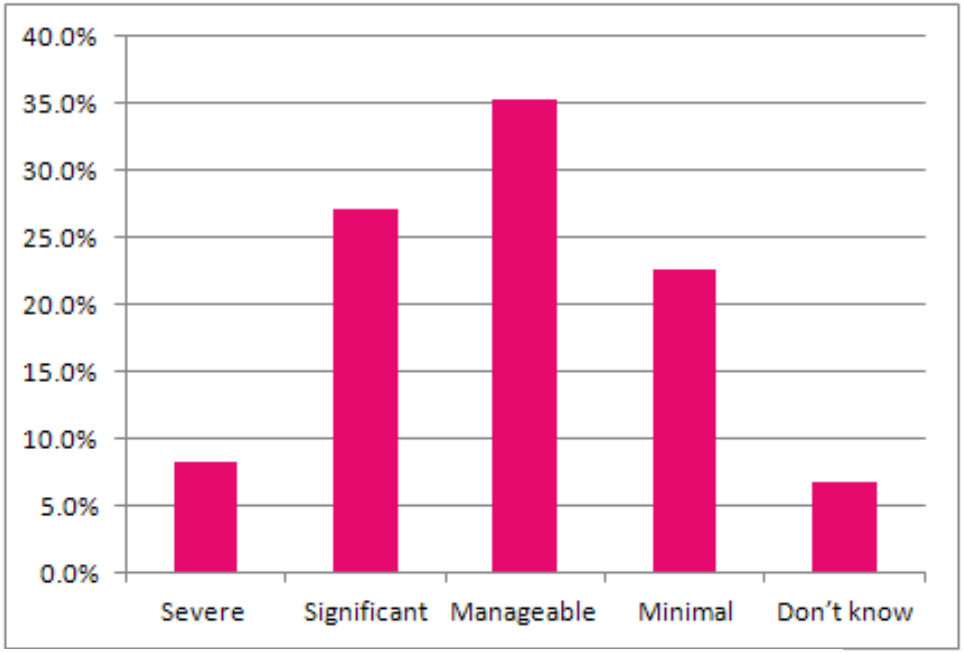


Chart Nine: Impact of Right to Object to Marketing

This may reflect an assumption that the right to be object would be exercised on the basis of an opt-out as currently happens already.

The effects of this existing right are known and understood, which may explain why there is limited concern

.

10. Measures Based on Profiling (Article 20)

1: Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

Article 20 protecting consumers from automated processing that might have an impact on them. This includes the use of personal preferences and behaviour, which raises an issue around web analytics as well as socio-demographics and other segmentations.

Profiling is one of the core activities within data management and marketing. At its simplest, it identifies the most appropriate targets for an offer or communication based on direct variables, such as age, income, products held, length of relationship, etc. Splitting a database between male and female customers would be a basic example of profiling that would identify personal preferences, for example.

Automated processing is an essential first stage in this profiling activity, given the volumes of data held by commercial and not-for-profit organisations. Rules are developed to split data sets based on business goals and the outputs from the profiling are then acted on operationally, for example, by using the selected individuals in a mailing programme or by setting the script for call centre agents based on a profile.

This activity has historically been invisible to the data subject. Explaining its purpose and value to them, such as ensuring they are on the most appropriate mobile phone tariff, would present a significant challenge. (This has already been seen in the difficulties found ensuring that consumers understand the use of cookies.)

This proposal would put marketers in a difficult position on two fronts:

1 - Gaining consent from data subjects would be difficult, costly and put at risk processes that are fundamental to efficient business and delivery of customer service;

2 - The nature of profiling covered by this Article, the level of automation involved and the legal effects considered to come under its scope leave significant scope for ambiguity and lack of compliance despite best efforts.

Consent for profiling should continue to be on the basis of opt-out, not opt-in, where this activity is being conducted outside of a contractual relationship (for example, where targets are profiled for marketing).

11. Responsibilities of data controllers (Article 22)

Extensive policies and implementation are required by this article, covering impact assessments, data protection officers, data security measures and documentation. Currently, these may be best practice, but are often an ambition for organisations, rather than a reality.

While nearly six out of ten organisations in the DQM Group Survey have specific security measures for personal data in place, a further third treat all data as if it was personal. Only a very small group (3.9 per cent) do not distinguish personal data from other types (see Chart Ten).

Data Protection Impact Assessments do not yet seem to be standard practice, with nearly four out of ten companies not completing these and a further third not sure if they do. Only one third of companies have formal risk assessment processes for their own collection and processing of personal data.

The biggest lag is around establishing key performance indicators for privacy, which 57.1 per cent have yet to do and 21.5 per cent are unsure about. A further gap is in the use of independent auditing of data protection and privacy processes, which just one third make use of.

However, there is a more positive picture in the realm of information systems, where privacy protection has become embedded at over half of companies. These businesses say it has become just part of the way they do things.

Contractual arrangements with third parties, such as outsourced data capture houses, database bureaux, telemarketing agencies and email broadcasters, would fall into particular focus under the new proposals. These service providers routinely handle data transfers from the data controller and therefore represent significant security vulnerabilities. It is critical to remember that the data controller retains responsibility for respecting a data subject's rights, even when

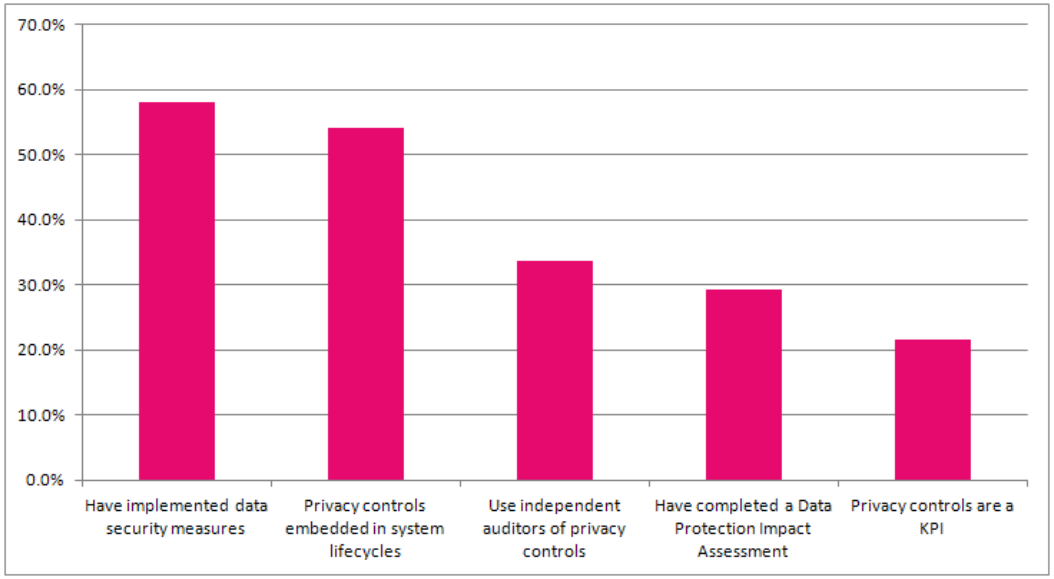


Chart Ten: Organisational Data Protection and Privacy Controls

personal information is being processed by a third party.

Although three quarters of organisations have comprehensive contracts with their third party data processors (see Chart Eleven), 7.9 per cent do not ensure these are always in place. Surprisingly, 15.8 per cent claim not to transfer data to third parties - the extent to which this actually happens through outsourcing may be invisible to some marketers.

Only half of these contracts insist that outsourcers have confidentiality contracts in place with their employees, creating a significant security gap. Minimum information security levels are mandated by contract in nearly six out of ten cases, but one in ten are not setting a benchmark that has to be met. Similarly, sub-contracting without written permission is not allowed by 58.9 per cent, but there are gaps elsewhere.

Auditing of compliance by third parties is lacking at 22.3 per cent of organisations.

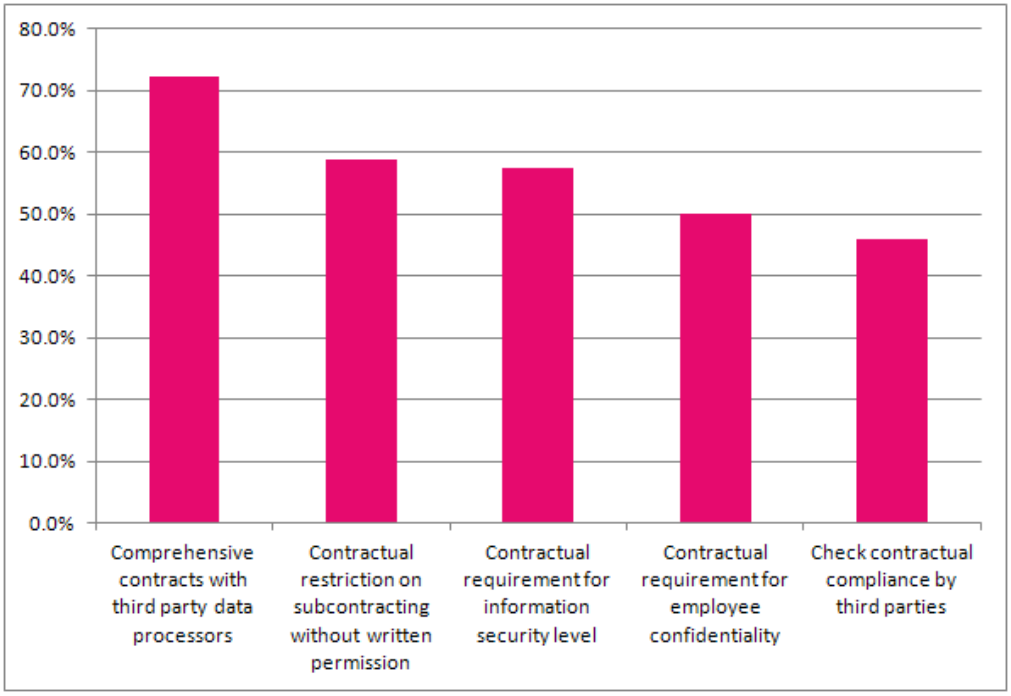


Chart Eleven: Contractual Arrangements with Third Parties

12. Notification of a Personal Data Breach (Article 31)

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority.

Most marketers already aim to notify the ICO of any significant data security breach and ensure mitigation of its impact as rapidly as possible. However, this proposal would need to be significantly better defined and clarified in order to be actionable. For example, a threshold for a notifiable data breach should be established in order to avoid excessive workload (and cost) for both the data controller and the national regulator. The issue of when "becoming aware" is defined, in particular, presents major concerns.

Notification of data breaches to national authorities, if desirable, would need to operate within clearly defined and limited parameters. It was certainly the case that respondents in the DQM Group survey expressed confidence in their data security, but the specific details of how they would respond to a data breach revealed fewer grounds for this confidence.

Confidence in the people, processes and technology being applied to control data security risks is positive overall, although with only around 60% confident or very confident there is clearly room for improvement (see Chart Twelve).

Written plans to identify breaches and notify any individuals affected are in place at 18.4 per cent of companies, with a further 18.9 per cent having some form of process or plan which is not documented. Four out of ten would work out what to do if they have to and 7 per cent have never even considered the issue.

It is notable that nearly two-thirds (64.7 per cent) or organisations do not have a budget for data breach notification and remediation, despite research showing that the average cost per record in a breach is around £64.

If a breach were to occur, 34.8 per cent believe they would be able to notify the ICO with details and a remedy plan within 24 hours. The

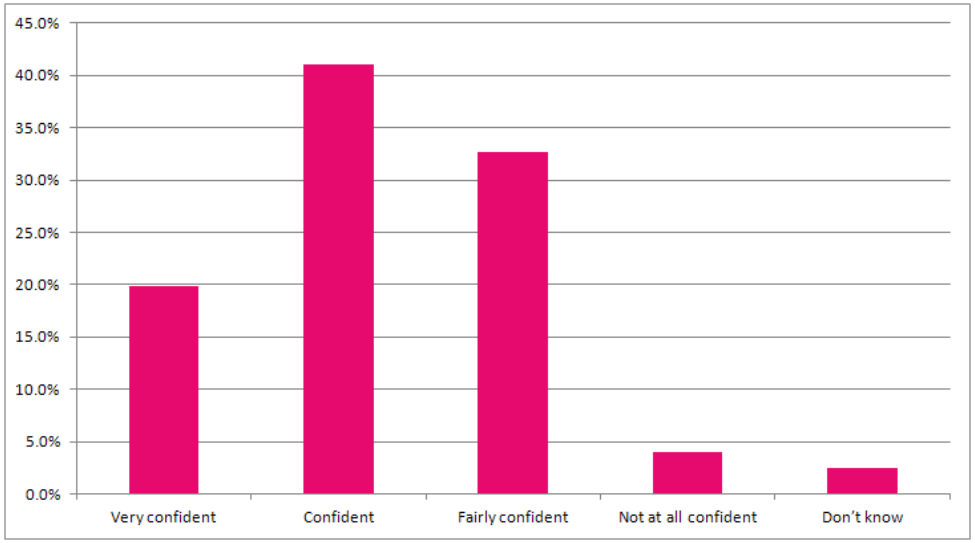
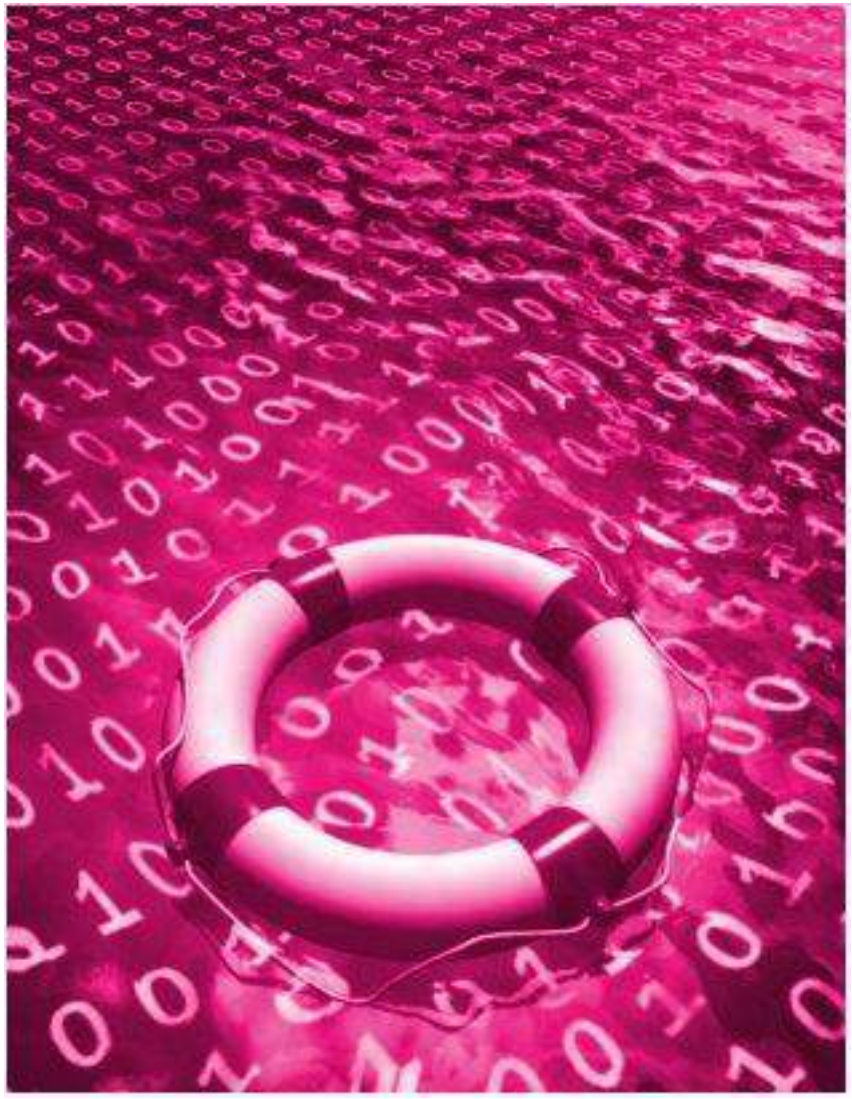


Chart Twelve: Confidence that Data Security is Fit for Purpose

majority (58.7 per cent) would have the ability to do this, but over a longer timeframe. Only 6.5 per cent would not be able to notify the regulator of a breach.

However, the majority (55.7 per cent) do not believe that notification will actually happen, unless the data breach is made public. One quarter expect notification over a longer timeframe, with just 6.5 per cent believing organisations would act within 24 hours. Significantly, 10.9 per cent do not expect organisations to even identify data security breaches.



13. Data Protection Impact Assessment (Article 33)

Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The concept of Privacy by Design - to ensure that new projects involving data capture, processing and storage respect existing data subject rights - is already becoming more widespread. Marketers also routinely consult with the ICO on the data protection issues they face.

An extension of this to a legal requirement to carry out impact assessments holds the potential to impose significant extra administrative burdens and costs. It could also lead to the potential "sabotage" of projects through vexacious complaints and objections by special interest groups (or even competitors).

This requirement needs to be constrained to a simple, documented process in which privacy impacts are reviewed internally and seek the views of data subjects within clearly defined parameters. As Chart Ten showed, only three out of ten companies have currently conducted a data protection impact assessment.

14. Data Protection Officers (Articles 35, 36, 37)

The controller and the processor shall designate a data protection officer…for a period of at least two years…and shall ensure the officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function.

Any organisation with more than 250 staff will need to appoint a data protection officer with expert knowledge of the area on a minimum two-year contract. Critically, this role has to be independent and must report directly to management as well as being the interface with the data protection authority. This would establish the DPO as a higher-status role than currently, where it is a role often shared with other duties which are potentially conflicting.

Designating a data protection officer incurs a cost and administrative burden on any data controller employing over 250 staff. This role often already exists within larger organisations who should be able to develop it into a standalone position independent of any influence. But there is a significant skills shortage in the marketplace which would make it challenging for every company to fill this role in the short term.

Data protection officers already exist in four out of ten organisations (see Chart Thirteen), although this is a role often performed alongside other responsibilities, which may not meet the demands of this proposal. A further three in ten companies told DQM Group that they had somebody capable of stepping into this role. But two out of ten would need to recruit and nearly one in ten expect to face difficulties. If implemented, this requirement would trigger a short-term lack of available talent which is likely to increase the number of companies facing difficulties.

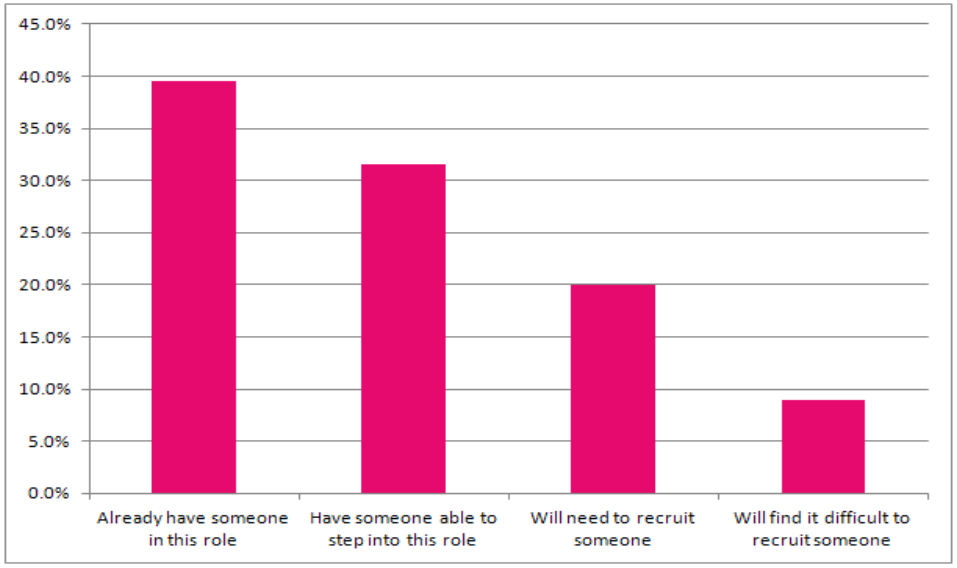


Chart Thirteen: Employing a Data Protection Officer

Action Points

- Conduct a data discovery exercise to identify where data is being stored and who it is accessed by and shared with.
- Review the data strategy for elements that are business critical and those which are optional or have a low impact on performance. Consider minimising data capture where possible in order to reduce reliance on potentially absent variables.
- Examine data capture notices and privacy policies for their accessibility to the consumer, ease of understanding and clarity about why data is being requested, the consequences of refusal, rights and controls, as well as future data sharing.
- Map all data sharing to create visibility of where personal information flows are occurring, both through outsourcing of activities to service providers and licensing of data to third parties.
- Document processes for handling requests to review, correct or delete personal information and examine the potential for automation or cost-reducing procedures.
- Identify data elements which are strictly the possession of the data subject and those which are the intellectual property of the organization - flag these to avoid including them in data portability requests.
- Strengthen data security policies and processes with clear documentation, lines of responsibility, budget and monitoring. Ensure that all data security requirements are understood and contractually enforced with third parties.
- Use an external auditor to examine data protection and security processes, identify strengths and weaknesses and to provide an action plan for improvement

About DQM Group

DQM Group is the leading provider of Data Governance expertise to the marketing industry, We specialise in research, audit and consulting services to both protect and maximise the value of our clients' most important asset – their customer data.

Why we're different – we deliver confidence in data.

DQM group is the only end-to-end Data Governance service organisation providing expertise in all areas of data management, whether developing effective data strategies, or addressing priorities in data security, regulatory compliance, data quality and insight.

Our consultants help leading brands including charities, media, telecoms and retail organisations understand their data capabilities and what they need to do to move towards optimal data governance.

Our proprietary automated secure data distribution and watermarking capability is truly unique and is 100% effective for identifying misuse . With our specialist audit know how it's probably why over 80% of all leading data owners, and increasingly major brands too, rely on our data risk management services.

We've extended our research and data intelligence capability through our range of Data IQ content products including the Data IQ Journal, in-depth Data IQ Industry Research Reports and regular events including the annual Data IQ Conferences held in May and October. These are all aimed at growing the use and value of data from a platform of best practice.

To register and receive your **free copy of the acclaimed quarterly DataIQ Journal** edited by leading data expert and industry commentator David Reed go to www.dqmgroup.com/dataiq

Together our difference is to deliver confidence in data to our clients

For more information go to www.dqmgroup.com or call +44 (0)870 242 7788.