Subject Access Requests: A Data Health Check

A RESEARCH WHITEPAPER

KATHERINE O'KEEFE, DARAGH O BRIEN

Castlebridge Associates | Invent Centre DCU Glasnevin Dublin 9 | www.castlebridge.ie

CONTENTS

INTRODUCTION

Subject Access Requests are often seen as a burden on organizations, taking up large amounts of time and resources. Organizations hold increasing amounts of information on individuals, and research shows that they often have difficulties responding to a data subject's request for access to the personal data held on them in a timely and efficient matter. This of concern to regulators, as many organizations fail to meet statutory requirements. However, this is symptomatic of larger breakdowns in information flows, data quality, and data protection compliance. Inadequate responses to access requests result in loss of customer trust and reputational damage.

But Subject Access Requests need not be a burden. Subject Access Requests are the canary in the coalmine, warning an organization of larger information problems or problems in processes that have in unwanted customer outcomes. The receipt of a Subject Access Request generally signals that individuals interacting with an organization have already had an unfavourable outcome or bad customer experience. Research shows that individuals are concerned about losing control over their personal information and their privacy rights. Claiming their right to access their personal data is one way that people assert control over their information. In fact, organizations are statistically more likely to have a Subject Access Request than a complaint about direct marketing. Organizations can use the Subject Access Request process as an opportunity to communicate with the people requesting access to their personal data to better determine the needs of their customers and how to meet them. This can uncover root causes of more than one problem.

Recent scandals involving data protection failures by charities in the UK shows the power of the Subject Access Request in revealing underlying problems in data use and data governance. Individuals and journalists are becoming increasingly sophisticated in using Subject Access rights to take control of their personal data and to discover possible violations of privacy rights.

The forthcoming EU Data Protection Regulation will introduce increased penalties for failing to provide the means for Data Subjects to exercise their right of access and for failing to provide the data when requested. These increased penalties create a strong driver for change, but there is a potential value-add benefit from broader improvements in Information Governance, Information Quality, and general Information Management capabilities.

An outcomes-focused holistic information strategy supported by Data Governance, Data Quality, and Data Protection will enable organizations to respond to Subject Access Requests efficiently and in a timely manner. Rather than seeing Subject Access Requests as a burden, an organization may use them as a health check and a chance to communicate with customers to identify ways to improve processes, outcomes, and customer experience.

WHAT SUBJECT ACCESS REQUESTS MEAN FOR AN ORGANIZATION

Under Section 4 of the Data Protection Acts, 1988 and 2003, with very few restrictions, any individual (or Data Subject) has a right to obtain a clearly explained copy of any data or information an organization holds on them, a description of the purposes for which it is held and to whom it may be disclosed, and the source of the data. People are becoming increasingly aware of this and taking advantage of their right to make Subject Access Requests. It is vital that organizations be able to meet these requests comprehensively and swiftly without placing undue burden on their resources.

The need to be able to respond to Subject Access Requests raises a challenge for organizations. The organization must have clear procedures and policies that staff can follow in the event a Subject Access Request is received. If an organization holds information about people in a "relevant filing system" (whether physical or electronic), it needs to be able to identify, locate, access, and provide clearly understandable copies of all the information related to a particular person in a timely manner. This can be a health check for an organization's data governance and management capabilities. If you do not know where your data is or how it is related to other data, it will be extremely difficult, costly, and time consuming to adequately respond to a Subject Access Request.

SUBJECT ACCESS REQUEST RESPONSE CAPABILITIES ARE NOT OPTIONAL.

The ability to respond to Subject Access Requests efficiently and in timely fashion is a necessary business capability. As the right of an individual to access personal data that an organization holds on them is enshrined in the EU Charter of Fundamental Rights, this is beyond a question of legal compliance but is a matter of upholding an individual's fundamental rights.

Yet, organizations, even organizations whose main concern is with protecting human rights, consistently fail to develop the ability to respond to an individual's request to access their data. As of the latest report from the Office of the Data Protection Commissioner, 54.3% of complaints to the DPC are related to failures to adequately respond to Subject Access Requests (521 complaints out of a total 960 complaints opened for investigation by the ODPC).

SUBJECT ACCESS REQUESTS ARE THE CANARY IN THE COALMINE

It might be is easy to see Subject Access Requests as a problem or a burden, but Subject Access Requests are not in fact the problem. Rather, the actions required to fulfil a Subject Access Request shine a light on information problems (and other problems) that businesses already have. Subject Access Requests can reveal underlying problems and trigger points in relationships with clients (or staff), and with data lineage, quality, as well as data protection issues, and processes for management and governance of data in general. As data is a valuable asset, these underlying

problems resulting in lack of proper asset management may well resulted in a significant unidentified cost to the organization.

Discovering these problems and instituting the processes and knowledge required to adequately respond to Subject Access Requests can improve the organizations data capabilities across the board and can also be an opportunity to better understand and improve client relationships.

WHY DO PEOPLE MAKE SUBJECT ACCESS REQUESTS?

From an individual's perspective, Subject Access Requests are one of the ways a person can exercise control over their privacy rights. Subject access rights have been described as the "cornerstone of the legislative protection of privacy," as they enable individuals to identify what data is held about them, how it is used, its accuracy, and the lawfulness of its use.[1]

Castlebridge Associates conducted a survey asking people who have submitted Subject Access Requests about their motivations and experiences. The findings are summarised in Figure 1 and Figure 2 below.

In terms of their motivations, the main reason given was simply that "it was their right to do so". The making of requests on foot of legal advice or on foot of an enforced Subject Access Request (where an employer required it) were not strong motivating factors for making requests. Tellingly, people were motivated to submit Subject Access Requests when they were in a dispute with an organisation, or when they believed the organisation had incorrect data about them. To a lesser extent, respondents reported being motivated by:

- Wanting to see how the organisation would react
- Receiving an unexpected/unsolicited communication
- Not trusting organisations of that kind.

This highlights the importance for organisations to recognise that when individuals are in dispute with you they will use Subject Access Requests as a tool in resolving that dispute. While it might be tempting for an organisation to presume that such requests might be vexatious, this is not a grounds for refusing to comply. The Data Controller may be able to point to some other relevant exemption in such cases (e.g. the information being covered by legal privilege), but a blanket refusal would be unlikely to be justified, except where the processing of the request required disproportionate effort.

It also highlights the importance of information quality assurance and information governance in the organisation as Subject Access Requests are motivated by unsolicited marketing contact and concerns about the accuracy of data held about individuals by organisations.

[1] Lorber, Steven. "Data Protection and Subject access requests." *Industrial Law Journal* 33.2 (2004): 179-190.

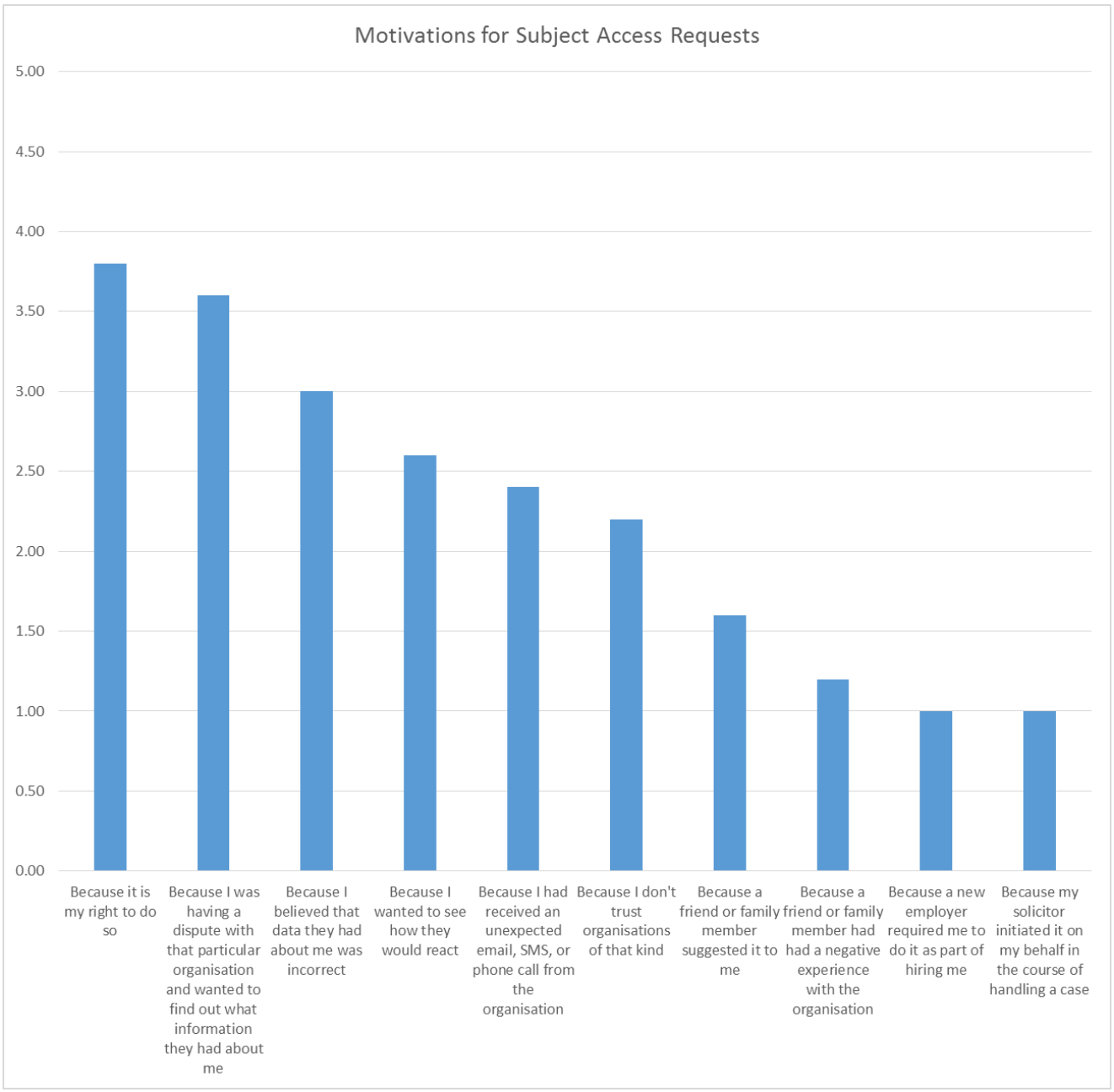


FIGURE 1 MOTIVATIONS FOR SUBJECT ACCESS REQUESTS (1 IS WEAK FACTOR, 5 IS STRONG FACTOR)

WHY DON'T PEOPLE MAKE SUBJECT ACCESS REQUESTS?

In our survey we also asked why people who hadn't submitted a Subject Access Request why they didn't. These broke down into two main groups: Those who hadn't considered using the Subject Access Request option and those who had considered it but had their issue resolved without needing to engage their full rights under the Data Protection Acts.

PEOPLE WHO DIDN'T CONSIDER SUBJECT ACCESS REQUESTS

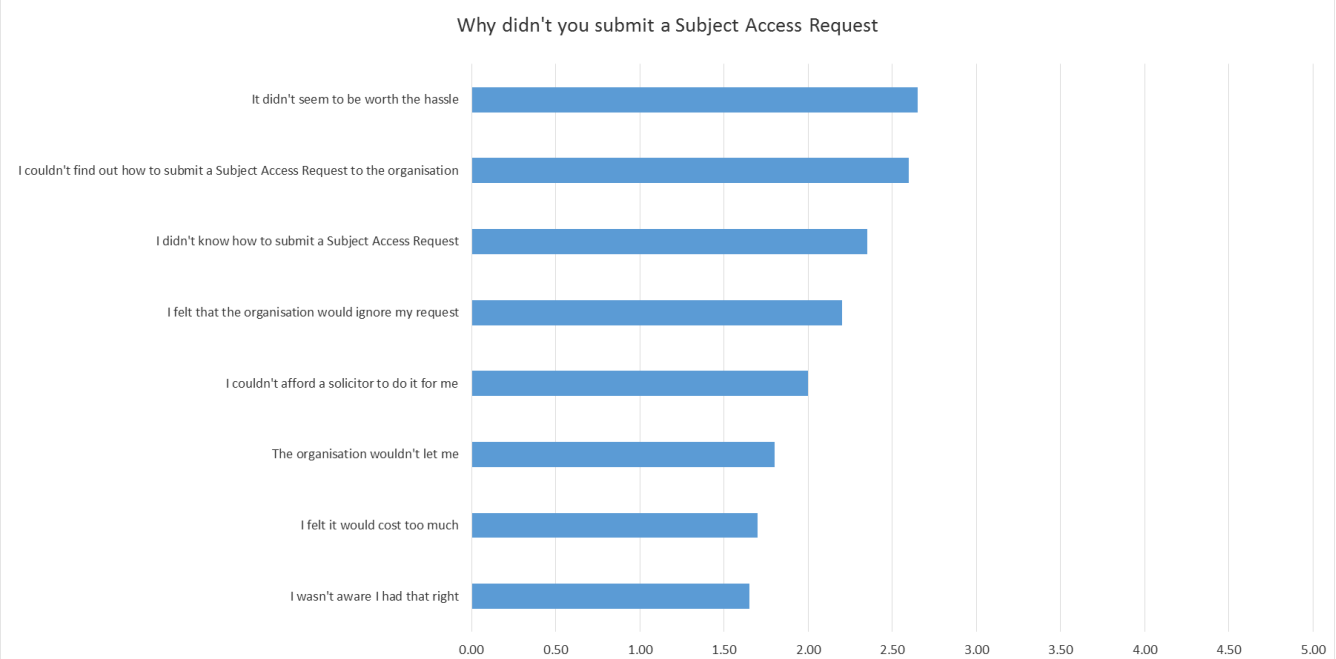


FIGURE 2 WHY DIDN'T YOU SUBMIT A SUBJECT ACCESS REQUEST? (1=LOW, 5 = HIGH)

The biggest reason people reported for not submitting a Subject Access Request was "hassle", followed closely by them "not being able to find out how" or their "not knowing how".

Subject Access Rights are fundamental rights enshrined in Article 8 of the Charter of Fundamental Rights. If organisations are not making it clear how people can exercise those rights, there is a failing on the part of the organisation. In Privacy Impact Assessments we have undertaken for clients, the ODPC has focused specifically on transparency and effective communication regarding the mechanisms by which Data Subject Rights, such as the Right of Access, can be exercised.

Providing access to data, and being open and transparent about how those rights can be availed of, helps to build and sustain trust between the Data Controller and the Data Subject. That is why it is a specific requirement of Fair Processing notices under Section 2D(2)(d) of the Data Protection Acts 1988 and 2003, which requires the provision of information "as to the existence of the right of access to and the right to rectify the data" provided by the Data Subject to the Data Controller.

Furthermore, the belief expressed by some respondents that their request would be ignored by the organisation, or that they required a legal representative to exercise this right on their behalf, while less highly rated as reasons for not submitting, are indicative of a lack of awareness of the existence of this right and the nature of the right on behalf of individuals. This, in turn, may be symptomatic of a wider lack of awareness of Data Protection Rights and Duties among individuals.

A good example of this lack of understanding and awareness arose in the media at the end of August 2015 when a man contacted a prime time afternoon radio show to seek their assistance in getting a copy of a recording of a 999 call during which a paramedic had talked him through delivering his own child. After nearly five years of requesting a copy of the recording, including writing to the Minister for Health and others, the father had resorted to asking a radio station for help.

At no time in the five year period did any member of staff in the HSE recognise the request that was being made as a Subject Access Request (suggesting a training issue with the HSE) and at no time was the individual made aware of his rights to make such a request to the HSE under Section 4 of the Data Protection Acts 1988 and 2003.

Ultimately awareness, or lack of it, would seem to be a key factor in the other factors which held people back from submitting subject access requests.

- "The organisation wouldn't let me" suggests that either an organisation wasn't aware of their obligations under the Data Protection Acts and Article 8 of the Charter of Fundamental Rights.
- "I felt it would cost too much" would suggest that individuals or organisations were unaware of the statutory maximum fee which can be charged.
- "I wasn't aware that I had that right" clearly indicates a lack of awareness of Data Subject rights.

We asked respondents who had not submitted Subject Access Requests if they would, if they found themselves in the same set of circumstances again.

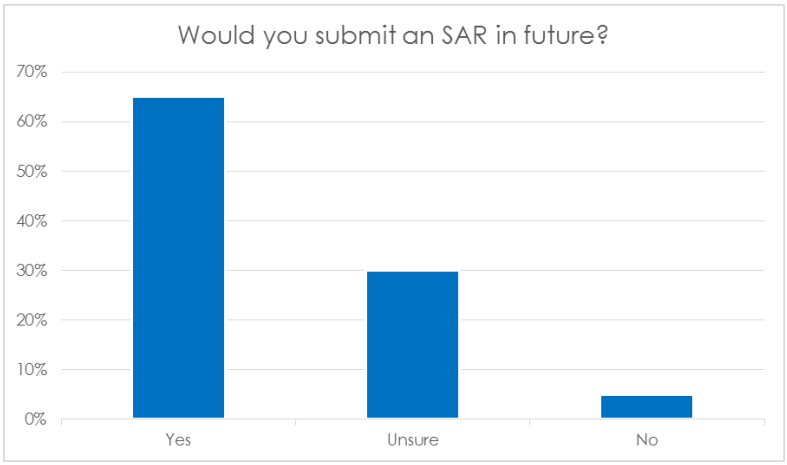


FIGURE 3 WOULD YOU SUBMIT A SUBJECT ACCESS REQUEST IN FUTURE?

Only 5% of respondents would not submit a subject access request in similar circumstances. In this context, we would suggest it would be advisable for organisations to look at their processes and procedures for identifying and addressing Subject Access Requests when they arise.

When we include people who had considered submitting a Subject Access Request but hadn't, there is still a very strong positive trend towards exercising fundamental rights of access to data:

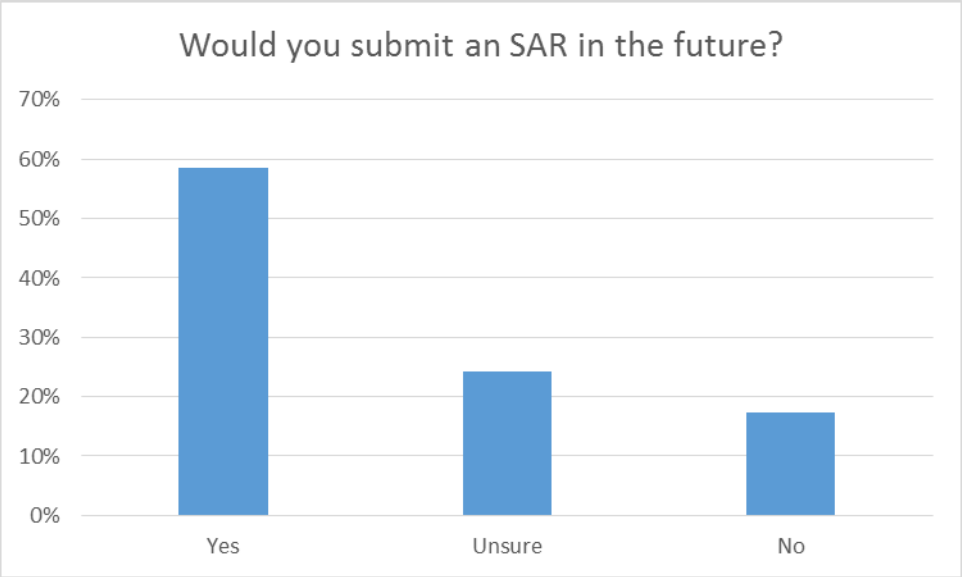


FIGURE 4 WOULD YOU SUBMIT AN ACCESS REQUEST IN FUTURE (NON-SUBMITTERS + CONSIDERED BUT DIDN'T)

THE IMPORTANCE OF ENGAGEMENT

When we asked survey respondents about their experience of having an issue resolved where they had considered submitting a Subject Access Requests, but had decided not to, the importance of well-defined processes and good engagement with Data Subjects becomes apparent.

- Over 20% of respondents who had **not** submitted Subject Access Requests reported that they had found the organisation had engaged with their issue in a timely and effective manner, removing the need for a Subject Access Request
- 11% of respondents highlighted the benefit of clear processes and procedures to in getting the information they had been seeking without having to proceed to a full Subject Access request.
- 11% indicated that their issue had been resolved by a staff member "showing them the information on screen".

While the latter cluster of responses indicates a well-meaning approach on the part of front-line staff, it does raise potential risks of unauthorised disclosure of other data, potentially including personal data about other individuals and may be indicative of a need for better training in some organisations.

For respondents who had submitted Subject Access Requests we asked how their experience of having their request processed would affect their recommendation of the organisation to a friend or colleague.

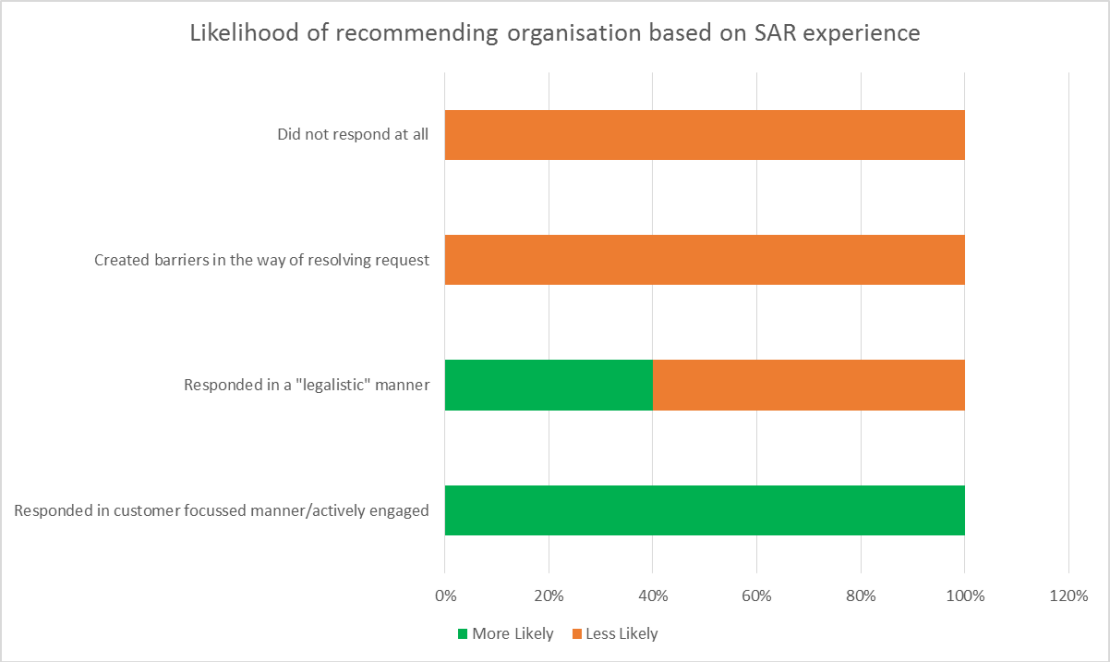


FIGURE 5 HOW LIKELY WOULD YOU BE TO RECOMMEND ORG BASED ON SAR EXPERIENCE

It is clear that a well-defined, customer focussed process for engagement is a key factor in turning the potential negative of a Subject Access Request into a positive experience for an organisation.

There is a correlation between the experience of those who submitted a subject access request and were engaged within an active and customer focussed manner and the experience of respondents who had considered submitting a Subject Access Request but had their issues resolved through good engagement and clear policies and procedures.

Castlebridge Associates advises all our clients to adopt a customer-centric approach to Subject Access Requests on the basis that any interaction with a data subject is an opportunity to develop your relationship with them. By having a customer focussed approach from the beginning of the process, opportunities may arise to reduce the scope of any subject access request or to resolve, in a non-confrontational manner, underlying issues that might have motivated the data subject to seek the information you hold about them.

Likewise, creating an overly legalistic manner in addressing Subject Access requests can also affect the quality of the engagement. While a certain amount of checks, balances, and controls should be in place in any SAR process, it is essential that organisations implement these controls in a way that is clearly explained to the data subject and are designed to be as "customer friendly" as possible.

WHO DO PEOPLE ASK FOR THEIR DATA FROM?

Our survey data shows some strong trends in terms of who individuals contact requesting copies of their data, or who people consider requesting copies of data from.

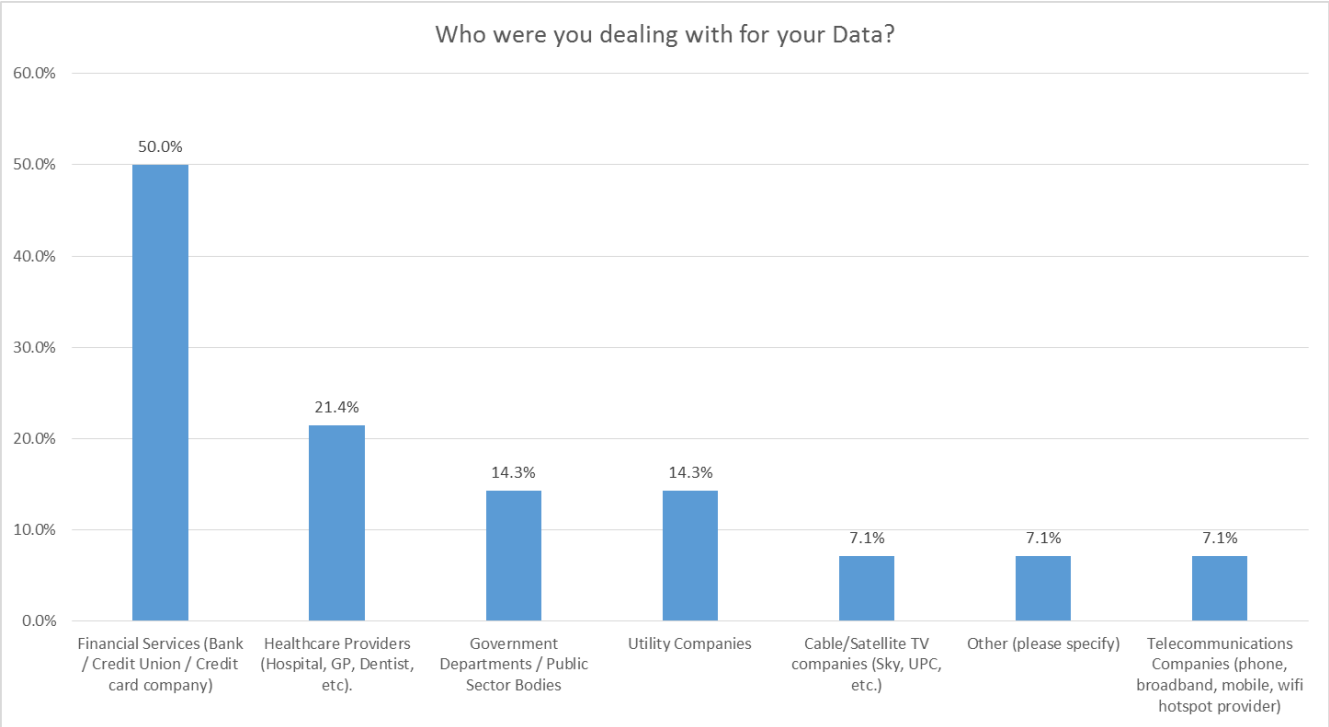


FIGURE 6 WHO WERE YOU ASKING FOR YOUR DATA?

Unsurprisingly, financial services organisations are the largest focus for Subject Access Requests. Healthcare providers are a distant second, with Government Departments and Utility companies being third. Given the recent media focus on matters of Government data processing and sharing, in particular the proposals to seek data from utility companies and cable television companies, this may change in the coming years.

However, there is a potential correlation of between the motivations for Subject Access Requests and the types of organisation who are approached with them: Subject Access requests to Financial Services companies with whom Data Subjects are, or may be, in dispute are not unexpected in the context of an economy that is only beginning to exit recession. This general desire to exercise some level of control over their 'data destiny' through the use of Subject Access Requests and other data subject rights is an understandable theme that is borne out by other research data.

A recent Eurobarometer survey [2] gauged public attitudes towards sharing their personal data and their concerns about the level of control they feel they have over their personal data and privacy rights. The survey results found that a large majority of

[2]TNS Opinion & Social network. *Special Eurobarometer 431 "Data Protection Report"* http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

people understand that sharing personal information is a necessary part of doing business and participating in modern life. However, they are very concerned about a lack of control over their personal data. Over two thirds (67%) of respondents expressed concern about not having complete control over their personal data.

Roughly 7 out of 10 people were concerned that organizations and authorities holding their personal data might use it for a purpose other than what it was collected for. In general, a majority do not trust private organizations and businesses to manage their personal information properly and protect their personal information. (While the EU Barometer survey results show a relatively high levels of trust in health and medical institutions and financial institutions, 56% don't trust shops and stores, and telecoms and online businesses are far less trusted. 62% do not trust landline or mobile companies or internet service providers; 63% do not trust online business.)

Public trust levels are directly affected by personal experience of previous customer experience outcomes. People are likely to use Subject Access Requests as a way to assert control over personal data when they feel they may have lost control or have had an undesirable outcome.

CONTROLLING ACCESS TO DATA: HOW DO ORGANISATIONS RESPOND?

In our survey we asked respondents who had submitted Subject Access Requests to indicate whether or not certain basic controls or instructions where in place or communicated to them in the course of submitting their Access Request.

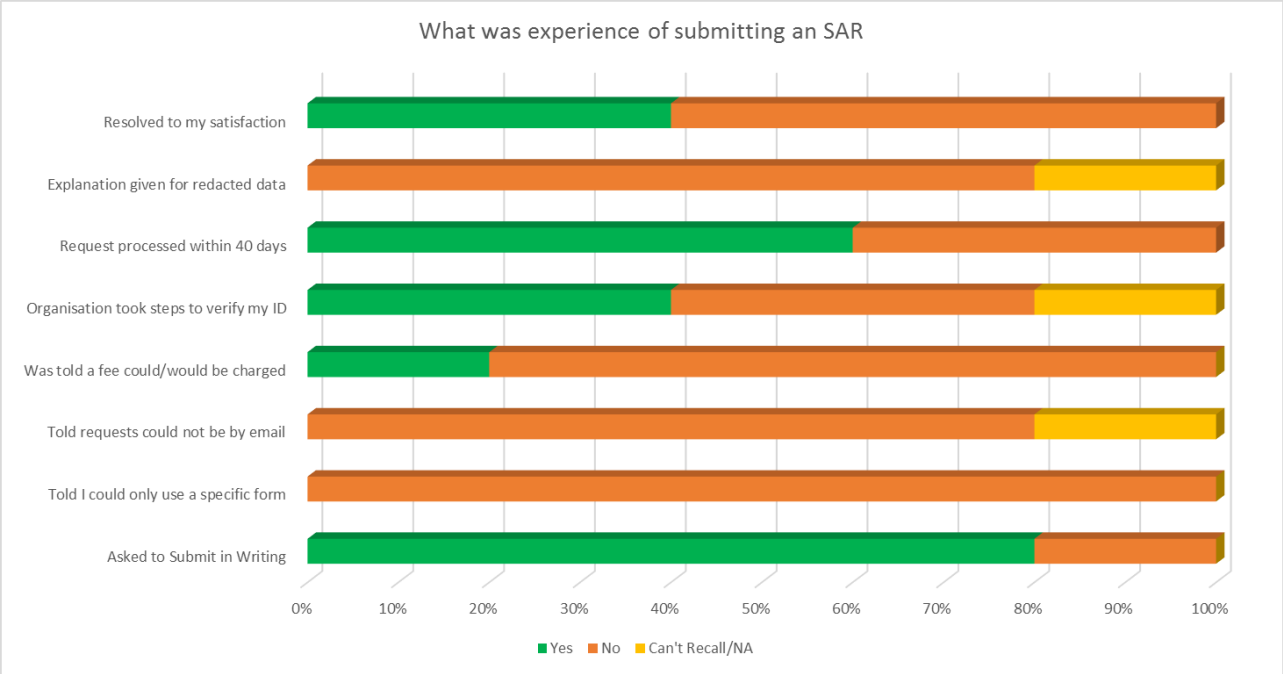


FIGURE 7 EXPERIENCE OF SUBMITTING A SUBJECT ACCESS REQUEST

It is interesting to note that, in our survey, only 40% of applications were resolved to the satisfaction of the Data Subject. This suggests that there is room for improvement in how Subject Access Requests are dealt with by organisations to improve satisfaction, even if the data being sought cannot be provided.

Worryingly, only 40% of organisations took steps to verify the identity of the person making the request. This means that 40% of Data Controllers are failing to ensure adequate technological or organisational controls to prevent unauthorised access to or disclosure of personal data as required under the Data Protection Acts. Seeking to verify identity is a good step to take to mitigate risks of unauthorised disclosure, and it also allows the organisation to commence a dialogue with the Data Subject to verify the scope of the request and, if necessary, identify underlying issues that might need to be addressed outside the scope of the Subject Access Request.

80% of organisations reportedly failed to provide any explanation for why data was redacted from the response. Just as organisations need to understand and respect the individual's right of access to data, individuals need to understand the limitations on that right. Organisations may be missing an opportunity to improve overall satisfaction levels with Subject Access Requests by providing a simple explanation about why data might be redacted from a subject access request. Such explanations need not go into specific detail but could simply address the scope of the exemptions to the Right of Access that might apply.

WHAT DO WE RECOMMEND?
Our recommendation to clients and delegates on our training courses is to have defined processes for dealing with Subject Access Requests that treat them as an opportunity to have a dialogue with your data subjects.

1. Engage in dialogue to verify their identity. Use data you have that would **not** be publicly available to verify their credentials. For example, you might ask what was the amount of their last transaction with you or the date of their last appointment.
2. Use the dialogue to verify the nature of their request. It may be possible to reduce the amount of data that needs to be provided through a discussion with the Data Subject. It may also be that a direct engagement with a human being might bring to light an underlying root cause for their access request that, once addressed, will cause the need for the access request to cease.
3. Confirm key process steps in writing
    a. Get the Data Subject to confirm their Subject Access request in writing. Email counts as a written form. Subject Access Requests can also come via social media (as they are in a written form)[3].

[3] For more on that point, see the ICO guidance on Subject Access Requests https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf, last accessed 01/Sept/2015

b. Confirm any discussions by phone with an emailed summary note. This is a record of what you have undertaken to do, what you have asked the Data Subject to provide, and what they have specifically requested from you.
c. Keep notes of all calls, communications, or meetings with the Data Subject as these may be necessary to establish reasonableness of your efforts or the vexatious nature of a request on behalf of the Data Subject.

4. Make sure all staff are trained how to recognise Subject Access Requests and you have a process to route requests from the point of entry to your Data Protection team as quickly as possible.

We also recommend that organisations conduct a cost/benefit analysis of collecting any statutory fee for a Subject Access Request. Bluntly, it can cost more than €6.35/£10 to process a postal order or cheque for that amount in terms of the allocated costs of manual processing, additional accounting effort etc. In one organisation, we calculated the Activity Based Cost for processing Subject Access Request fee at between €15 and €20 per request.

Given that the statutory fee will be removed in the Data Protection Regulation, and the Irish DPC has been clear that non-payment of the fee should not delay the commencement of work to comply with the Subject Access Request, organisations should consider either using an automated process (e.g. a PayPal account) or simply waive the fee.

It is important that your organisation's policies and procedures for Subject Access Requests address issues such as:

- Requests by 3rd parties on behalf of a Data Subject
  - Examples: Solicitors, Next-of-Kin with Power of Attorney
- Requests for information about children
  - Rules regarding Parents/Guardians
  - Rules regarding Grandparents/Extended family
  - Rules regarding Court Orders or other similar issues
  - Capacity of the child to make decisions about their own data

THE TICKING CLOCK

Within all of this, the organisation also has to consider the limitations of the 40 day window to respond to requests. This will involve collating the data, reviewing the data, redacting data, and then packaging it for onward distribution to the Data Subject, so the sooner you *start* the sooner you *comply*.

A key challenge will be locating and categorising data. This is why an effective Information and Data Governance programme, with appropriate metadata management and document management is essential to effective compliance.

SUBJECT ACCESS REQUESTS ARE AN OPPORTUNITY NOT A BURDEN

If we consider Subject Access Requests in the context of the wider set of outcomes an individual may seek from their dealings with an organisation, the receipt of a Subject Access Request can be a warning sign, highlighting the presence of a trigger point causing an unfavourable outcome for the individual. Or it can be an opportunity to provide an additional service to add value.

Whether it is the customer of a bank seeking to know what the bank knows about them before they go to renegotiate the terms of a loan, or the father who just wants to be able to play his child the recording of his input into bringing them into the world, the real reasons for the request can be many and varied. Intelligent organisations need to identify and capitalise the opportunities while ensuring they can identify and mitigate risks as well.

This means that a Subject Access Request is also an opportunity for communication to improve customer experience. At an external customer outcomes level, the Subject Access Request is an opportunity to reach out to the person who made the request and find out what outcome they are looking for and how their needs might be met. Knowing these things can help an organization respond more effectively to the wants and needs of their clients.

Subject Access Requests are a necessary capability that can be used to an organization's advantage to improve information outcomes and customer experience. While failing to adequately respond to Subject Access Requests can cause reputational damage as well as legal difficulty, proactively responding to Subject Access Requests may create a reputational and competitive advantage. Subject Access Requests are a point of communication that can be used to improve information outcomes and overall customer experience.

One simple response is to pick up the telephone and call the individual who submitted the Subject Access Request, to learn more about their individual needs and how the organization can best facilitate the fulfilment of their needs. This may result in a more fine-tuned request or in discovering the root cause of the customer's dissatisfaction. In doing this, an organization may be able to analyse how to improve their processes or communications, using the knowledge gained to ensure more favourable customer outcomes in the future.

Of course, care must always be taken not to disclose personal data inadvertently. That is why effective processes, procedures, and controls for handling Subject Access Requests are essential. Within that, the organisation must ensure that staff are appropriately trained to identify Subject Access Requests, understand the implications of them, and respond to them correctly. One approach we recommend to clients is to run "Access Request Drills" to practice the steps of processing requests and to ensure all participants know their role. We also suggest 'mystery shopping' your organisation to see what the individual's experience is of engaging with you.

You may be unpleasantly surprised.

CASE STUDY: THE RESULTS OF A SINGLE SECTOR "MYSTERY SHOP"

To adequately respond to a Subject Access Request, an organization must be able to identify and locate all relevant information and files, determine what is personal information and any relevant exemptions, make any necessary redactions, and produce the requested information in a timely manner. This requires adequate knowledge of legislation, knowing and understanding the purpose for using and retaining the data held, and clear communication as well as the ability to find the relevant data. If an organization lacks adequate data governance and a holistic information strategy, the lack of quality information or breakdown in information flows can cause a failure to adequately respond to a access request. This may result in the perception that the organization is deliberately hiding a person's information from them, in spite of the organization's best efforts. In effect, customers are sitting on a stool to have it collapse underneath them. If this happens, individuals will be likely to lose trust in an organization's ability to treat their personal data properly or to understand or care about their fundamental rights.

Castlebridge Associates, in conjunction with a partner in the relevant industry sector, completed a "mystery shop" submitting Subject Access Requests for data to 20 organizations.

THE RESULTS

Over half of the organizations failed to provide a complete response to the Subject Access Request.

Some responses were immediate, but similar to the experiences described in the IRISS research, many responses took multiple emails. At the end of the 40 day period, less than half of the organizations had responded to the request by providing data. Of those, many had made some serious errors in processing the requests.

DO YOU KNOW WHERE YOUR DATA IS?

DO YOU KNOW WHY YOU HAVE THAT DATA?

DO YOU KNOW WHY YOU *STILL* HAVE THAT DATA?

CAN YOU EXPLAIN IT TO A CUSTOMER?

Although many organizations decided not to charge a fee to process the request (an optional fee of no more than €6.35 is provided for under the Acts), most of the organizations who decided to request a fee charged the wrong amount, in effect using an illegal fee as a barrier to an individual's right to access their own information.

Disturbingly, most organizations that responded to the request did not take steps to verify the identity of the individual requesting their data. This means the organizations shared personal data without any checks or controls in place to ensure the recipient had the right to

access that data. Such an action violates the fourth principle of the Data Protection Acts, which states that a data controller must keep personal data Safe and Secure, having appropriate measures in place to prevent unauthorised access to or disclosure of personal data.

At the close of the survey, well after the 40 day statutory period, 40% of the responses were still pending completion and 6% of the organizations contacted had yet to respond at all.

% Completed	46.67%
% Requesting ID	6.67%
% Requesting Fee	20.00%
% Requesting CORRECT fee	13.33%
% of responses pending completion	40.00%
No Response	6.67%

THE OUTCOME: WHY IT MATTERS

The results of this survey suggest that the majority of Irish organizations lack the capacity to comply with the law when faced with a Subject Access Request. The errors in responding to Subject Access Requests demonstrate both inadequate information governance and a lack of training in understanding an organization's duties as a data controller under the Data Protection Acts. Without clear training in how to respond as well as Data Governance, Data Quality, and Data Protection as strong supports for a good information outcome, producing an adequate response to a Subject Access Request within the statutory 40 day period is likely to be very difficult for an organization.

However, this difficulty also presents an opportunity. Any trouble in responding efficiently to an access request is a warning symptom is a warning symptom, highlighting a blockage or corruption in the organization's information flow or processes that need improving. At an internal outcomes level, this points out an opportunity to do a root cause analysis and find out where the problems lie.

SUBJECT ACCESS REQUESTS, OUTCOMES, AND REGULATORS

Ultimately, when organisations fail in their obligations under the Data Protection Acts or Directive, they will complain to Regulators. Both the UK's ICO and the Irish ODPC have reported increases in the volume of complaints arising from Subject Access Requests in recent years.

Of course, Regulators are one route of complaint when an organisation fails to live up to its obligations. Increasingly, Social media is an outlet where failings can be aired publicly.

WHY DO PEOPLE COMPLAIN TO THE DATA PROTECTION COMMISSIONER ABOUT SUBJECT ACCESS REQUESTS?

The Data Protection Commissioner's Annual Report for 2014 outlines more than one case study regarding failure to properly respond to Subject Access Requests. It notes a "common theme emerging from the complaints" of lateness in processing the access request. The report describes three related situations of increasing severity:

- The Subject Access Request is not processed within the statutory 40-day compliance period
- The data controller fails to acknowledge receipt of the access request within the 40-day period.
- The data controller has taken no action to process the request until the Office of the Data Protection Commissioner investigates a complaint against them.

As in all of these cases the Data Protection Acts have been violated, the Office of the Data Protection Commissioner has expressed deep concern about the prevalence of this offence.[4] Access rights accounted for **54%** of complaints made to the Data Protection Commissioner in 2014.

Unhappiness with responses to Subject Access Request are also a major cause for complaint in the UK. According to the 2014/15 Information Commissioner's Office, **46%** of the 14,268 data protection concerns raised in the year were related to Subject Access Requests.[5]

INADEQUATE RESPONSE TO SUBJECT ACCESS REQUESTS IS A EUROPE-WIDE PROBLEM

This failure to adequately respond to Subject Access Requests is not limited to Ireland and the UK, but is a Europe-wide problem.

The University of Sheffield led a cross-European comparative analysis of data access rights that tested people's practical access to their rights of data access in the contexts of data protection legislation and its implementation by organizations across ten

[4] Annual Report of the Data Protection Commissioner of Ireland Presented to each of the Houses of the Oireachtas pursuant to section 14 of the Data Protection Acts 1988 & 2003.
[5] Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements*2014/15, p.14

European Union member states (Austria, Belgium, Germany, Hungary, Italy, Luxembourg, Norway, Slovakia, Spain and the United Kingdom). Researchers submitted access requests to data controllers, asking for copies of their data and information on how their data was processed and any information regarding sharing of their data to third parties. The researchers encountered difficulties at nearly every stage of the Subject Access Request process. Across the study, over half (57%) of the requests resulted in "negative outcomes", ranging from inadequate query responses to non-disclosure of personal data.[6]

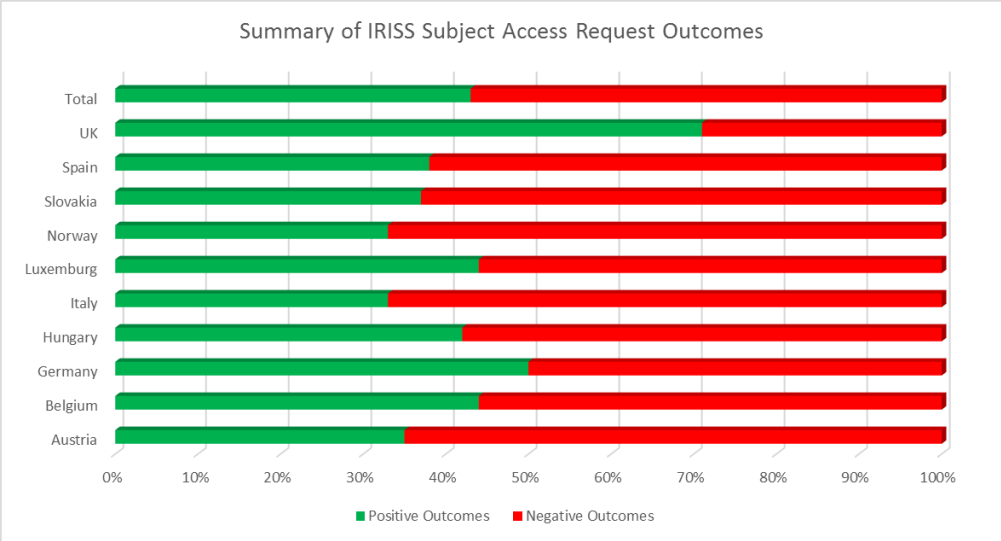


FIGURE 8 SUMMARY OF FINDINGS REGARDING THE RESPONSES RECEIVED TO SUBJECT ACCESS REQUESTS

> "Across the entire study, less than half (43%) of all applications resulted in a positive outcome. In the majority of cases therefore (57%), some aspect of researchers' requests was answered inadequately. This ranged from non-disclosure of personal data to receiving inadequate responses to queries regarding third party data sharing practices or the use automated decision making processes."

Interestingly, while the UK Information Commissioner's Office annual report found that nearly half of its concerns related to Subject Access Requests, the IRISS study found the UK had most positive outcomes of the countries in their study. Among other things, the study identified "facilitative practices" where organizations tried to help individuals access their data, enhancing transparency.

This echoes the findings of our survey with respect to the need for customer-focussed and defined approaches to dealing with Subject Access Requests.

[6] Galetta, Antonella et al. *Mapping the Legal and Administrative Frameworks of Access Rights in Europe – A Cross-European Comparative Analysis.* IRISS project Work Package 5. University of Sheffield, 2014. http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Summary-Meta-Analyses-for-Press-Release.pdf

WHAT DOES IT MEAN? IMPLICATIONS FOR ORGANISATIONS

Data Subject Access Requests are a fundamental right of Data Subjects (i.e. your customers, employees, etc.) under Directive 95/46/EC.

- It is a right that people are not always aware they have
- It is a right that, when people realise they have it, they are likely to use it
- It is a right that people will exercise despite "hassle" or barriers. However the ease of access to the right and the experience people have getting access to their data from organisations directly effects their perception of the organisation.
- Across Europe, most data subjects have negative outcomes when they attempt to exercise their Subject Access rights.

THE GREED MOTIVE

If we consider respect for privacy rights to be a source of competitive advantage for organisations, it is clear that there is a significant market opportunity for organisations who improve the experience people have when seeking to get copies of information held about them by an organisation.

Organisations that invest properly in the information management infrastructure and processes necessary to comply with Subject Access Requests more quickly and easier will reduce the cost of compliance to them, and will create a trust-based advantage that their competitors will need to match.

Not only that, but organisations that have adopted a customer-focused approach to Subject Access Requests tend, in our experience, to see the Data Subject as just another customer in the line of potential internal and external consumers of that personal data (albeit a more privileged one). They realise that the difficulties, delays, and barriers to effectively providing data to the Data Subject are likely occurring in other processes. They realise that those challenges represent avoidable costs in their information supply chain and seek to remove them.

In the context of the "Greed motive" for organisations, Subject Access Requests represent a good 'canary in the coal mine' to flag potential issues with the system of Governance for processing personal data.

- Do you know where all the data is?
- Is it classified correctly?
- Are you able to remove or redact data easily from data sets when giving it to 3rd parties?
- Can you anonymise data easily when giving it to third parties?
- Do you know where your data flows from and to?
- Do you have conflicting copies of the same data?
- Do you have duplicate data about people in your systems? If yes, is that for a valid purpose or is it an avoidable cost?

THE FEAR MOTIVE

In our survey, only 42.8% of respondents had submitted a Subject Access Request or considered submitting one. 58.2% of respondents hadn't. Only 21.4% of respondents had actually submitted a Subject Access Request.

When 21.4% of a population avail of a right which organisations mishandle between 46% and 57% of the time, this represents a significant challenge for organisations with the imminent arrival of the EU Data Protection Regulation.

Article 15 of the draft text sets out (largely irrespective of which draft you read) extensive requirements for data to be provided to Data Subjects under an Access Request. Overall, this echoes the current requirements in Directive 95/46/EC and the Data Protection Acts, with some additional requirements. Data Controllers will be required to provide:

- The data itself
- The purposes of processing
- The categories of data concerned
- The recipients or categories of recipients that data is shared with or disclosed to
- Retention periods for the data
- Information as to the source of data if not obtained from the Data Subject
- Meaningful information about the logic involved in any data processing and the envisaged effects of such processing, at least in the case of profiling.
- Safeguards applied to transfers to third countries

Article 12 requires that Data Controllers establish clear procedures for providing information and for allowing for the exercise of data subject rights, including the right of access. Article 12(2) requires response "without delay" and may reduce the period for response to one calendar month from the current 40 calendar days.

Article 79(4)(a) may impose a fine of up to €250,000 or 1% of global turnover for failing to have a mechanism for people to submit Subject Access Requests and for not responding promptly or in the required format.

Article 79(5)(b) may impose a fine of up to €500,000 or 2% of global turnover for failing to provide access to data to a Data Subject.

Currently, up to 57% of Subject Access Requests filed in the European Union have a negative outcome in which they fail in some way to meet the required standards. This represents around 20% of the potential population of data subjects who might file subject access requests.

The proposed penalties create a strong business driver for organisations to take a look at their processes from the Data Subject's perspective and ensure:

- They have a simple and easy to use mechanism to request data
- They acknowledge and respond promptly
- They provide the required information as quickly as possible.

SATISFYING FEAR AND GREED

Organisations need to adopt a strategic approach to Subject Access Requests that sees them as a key function in the organisation, and recognises the importance of the data subject as a key stakeholder in the processing of personal data in the organisation.

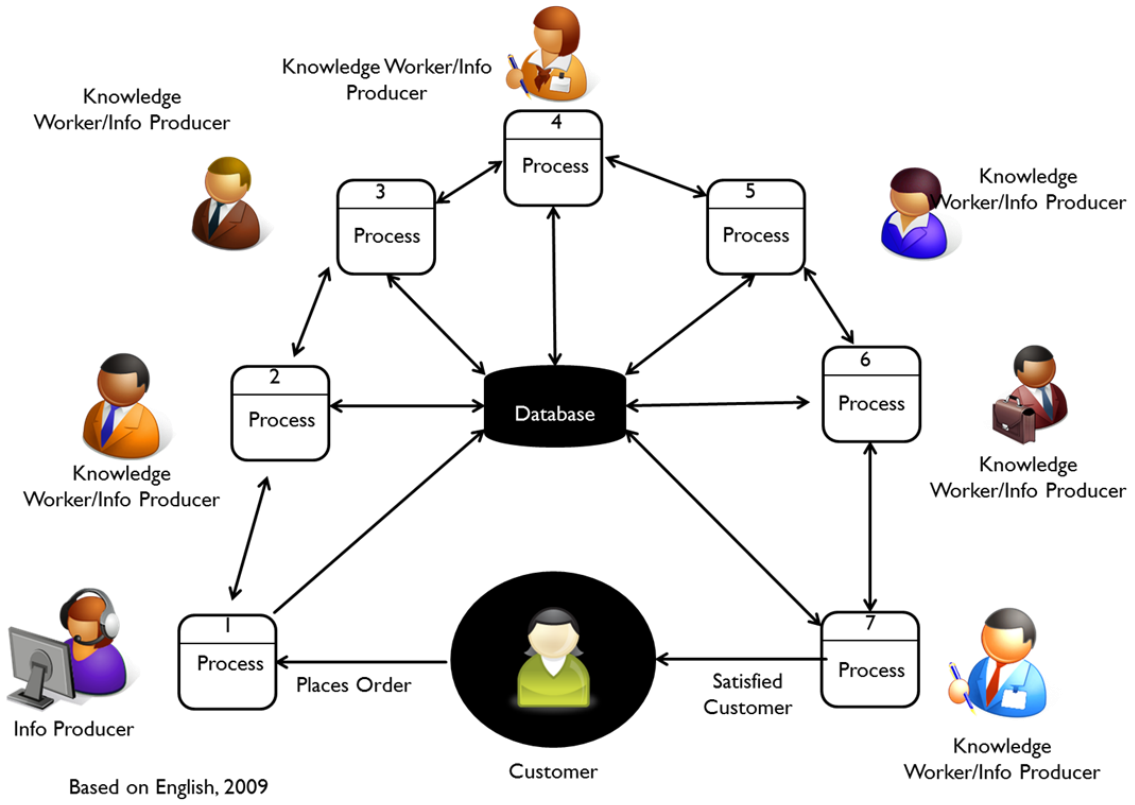


FIGURE 9 THE INFORMATION VALUE CIRCLE

By considering the Data Subject as a stakeholder, the organisation can begin to identify the flows of information that affect the Data Subject, ensure that the processes for making Subject Access Requests, or for making data available to the data subject through user portals or other mechanisms, is easy for the Data Subject to use, and not just your developers.

By adopting a "customer-centric" approach to the Data Subject, the organisation can start to build sensible interactions that will support the control checks of identity validation and verification, but will also be able to consider the wider Information Value Chain in the organisation and improve it as part of improving their basic compliance capability.

Organisations that continue to keep customers out with complex processes will inevitably lose out either in the Greed motivators (customers will trust competitors more) or in the Fear motivators (they will fall foul of the General Data Protection Regulation)

UNDERSTANDING SUBJECT ACCESS REQUESTS THROUGH INFORMATION GOVERNANCE

Organisations need to develop more strategic thinking about Subject Access Requests, and Data Protection in general. In particular, people in organisations need to start thinking differently about Subject Access Requests and about the relationship of Data Protection to other critical disciplines such as Information/Data Governance and Information/Data Quality.

Ultimately, everything is about outcomes. The quality of the Data Subject experience, and the assessment of the Supervisory Authority of the suitability and effectiveness of your Data Protection controls are both driven by how well the outcomes you deliver meet or exceed the expectations of internal and external stakeholders in your organisation.

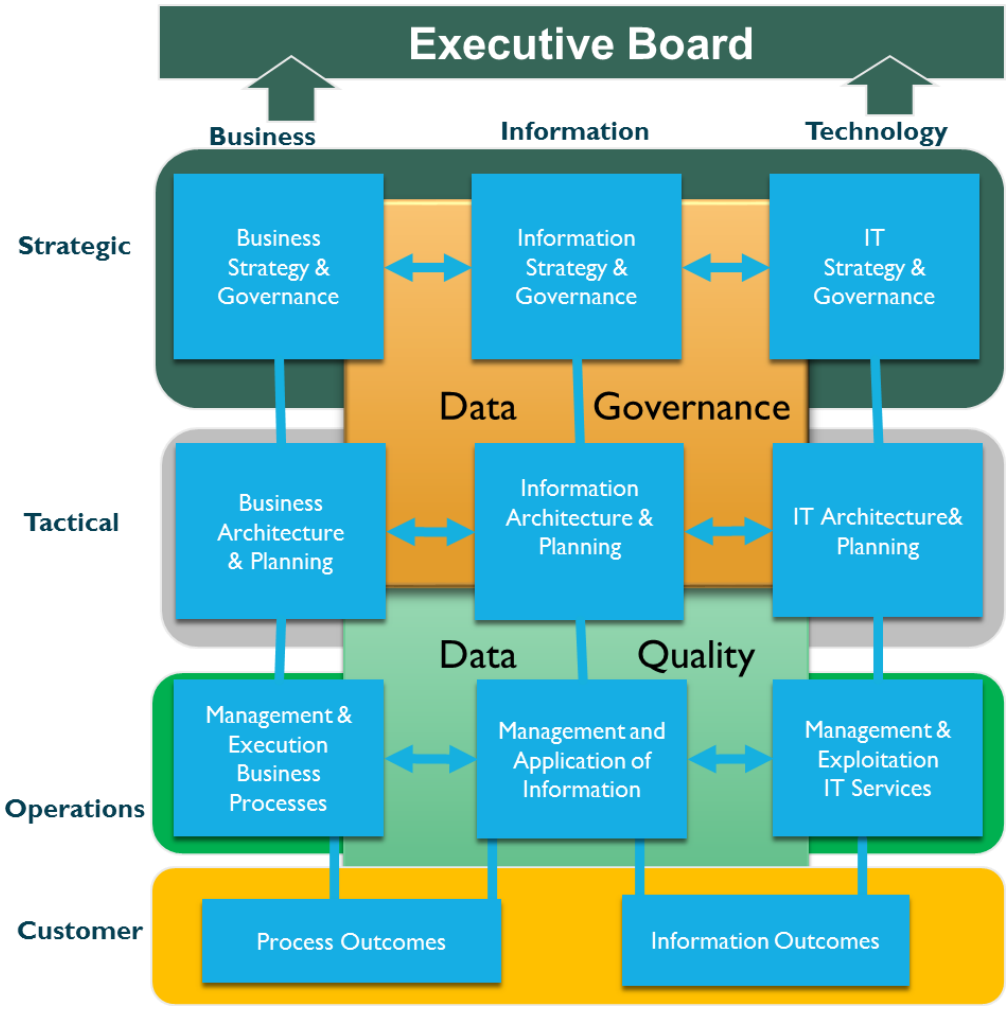
THE 11 BOX MODEL AND OUTCOMES-BASED THINKING

Failing to adequately respond to a Subject Access Request is an undesirable outcome, often resulting from a breakdown in information flow or poor quality information. A piecemeal, silo-based approach to information in an organization will often result in key dependencies being missed or sub-optimal delivery of required outcomes. A holistic perspective on and strategy for information is necessary. It is essential that organizations develop a clear focus on outcomes in their data and technology implementation strategies. This extends throughout the business and technology dimensions of an organization, as information is the life-blood of an organization, flowing through and bringing life to the organizational body as a whole.

Castlebridge Associates propose a simple 11-box model through which organizations can develop a holistic perspective on the development and execution of effective Business, Technology, and Information strategies that are aligned with supporting clearly defined Process and Information Outcomes for the providers of healthcare services and the recipients of those services.

This model is based on a framework for strategic Information Management change developed by Professor Rik Maes and his team in the University of Amsterdam. The original model identifies that there are three layers in an organisation that need to be considered: Operational (frontline), Tactical (Line management), and Strategic (Senior Executives). The organisation needs to ensure effective alignment of capabilities across three verticals: Business, Technology, and Information. Historically, organisations have focussed on Business and Technology capabilities without explicitly considering the Information Capabilities that are required.

We extend this original framework by including the customer's perspective, driven by Process Outcomes (did the process achieve the objective) and Information Outcomes (was the right information available to achieve the objective). This allows us to map the organisation's operational, tactical, and strategic capabilities to key customer outcomes and ensure alignment.



Data Protection compliance, including the ability to comply with Subject Access Requests in a timely and effective manner, requires an effective alignment of Business Governance, Information Architecture, and Technology service, along with appropriate business processes and Information Governance.

For example: if your organisation does not have a mechanism to detect Subject Access Requests and direct them to the appropriate co-ordination point, you may face a significant fine due to not meeting the required time frame for completing the request. This requires an alignment of:

- Business Processes ad Operations level
- IT Services for communication of the request
- Information Planning to ensure the right persons get the request
- Information Governance to ensure the right decisions are taken about the request.

THE "THREE LEGGED STOOL" AND SUBJECT ACCESS REQUESTS

Data Governance, Data Quality, and Data Protection are three main supports that uphold the overall information outcomes for a customer experience. In essence, these are three legs of a stool.

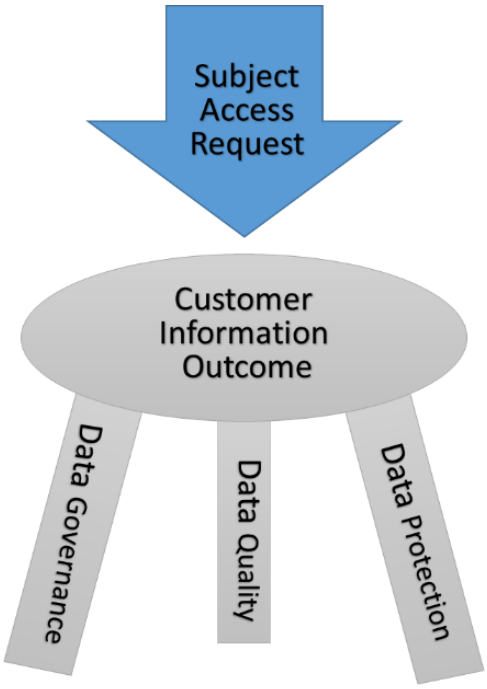


FIGURE 10 THE THREE LEGGED STOOL

Whatever an individual's motivation for submitting their request, Subject Access Requests are essentially a way in which the customer can apply pressure, making sure all three legs are functioning correctly, ensuring a stable information outcome that supports their rights. The failure of any one of the three legs results in an unfavourable experience.

Unfortunately, it is often the case that he stool is broken and the organization fails to produce an adequate outcome.

If we assume that the 'seat' of the stool is the Information Outcome that the Data Subject is seeking, then the organisation needs to ensure that there is appropriate alignment of and integration of Information/Data Governance, Information/Data Quality, and Data Protection capabilities.

INFORMATION/DATA GOVERNANCE

Within the organisation is there a function who will co-ordinate the processing of the subject access requests?

How is the data in the organisation classified and categorised? Is it possible to quickly identify all the databases, fields, files, and records that contain personal data or other categories of relevant data? Who decides the relevance on a case by case basis? Where exceptions or exemptions might arise, who evaluates and decides on this?

Across the organisation and its Data Processors, does each functional area understand their role in relation to Subject Access Request responses? Do they understand the importance of timely and complete responses to internal requests for information? Is the Subject Access Request response team empowered to require responses, or compelled to ask nicely and hope for the best?

INFORMATION/DATA QUALITY

Personal data provided to Data Subjects on an Access Request must be provided 'as-is' in the database or file, with any abbreviations or field names etc. being explained and the general logic of any algorithms or derived data also being explained.

Does your organisation measure the quality of data? Does it measure the consistency or completeness of the data you are processing? Do you conduct any assessments of

the accuracy of the data? Do you perform data health checks on data you obtain from third parties? When conducting data matching exercises, do you validate the accuracy of the matching? Do you have mechanisms in place (via your Information Governance structures) to react promptly and effectively to any reports of poor quality data, missing data, or mismatched data in your organisation?

Of course, Information Quality goes further in terms of the quality of your underlying data models: Are they complete? Do they have place holders for irrelevant information? Are you capturing data at a level of granularity that is not needed for your purposes?

Finally, Information Quality metrics can allow you to assess your level of compliance with key Data Protection principles such as validity of consents for direct marketing – have you contacted them all in the last 12 months or not?

DATA PROTECTION

Finally, the third leg of the stool is the understanding of Data Protection principles and legal requirements in the organisation. Knowing the rules is essential to being able to implement them through efficient governance and demonstrate the effectiveness of said governance through appropriate quality metrics and KPIs.

Furthermore, detailed knowledge of the applicable exemptions and exceptions, and a radar for changes in legislation or legislative interpretation with an understanding of how that will affect your Information Governance processes, is essential to keeping the three legs aligned and stable.

Focussing on any one of the three legs however will give rise to an unstable platform on which to rest the customer's expectations about the information outcomes that should be delivered through the Subject Access Request process.

This is why up to 57% of Access Requests across Europe lead to negative outcomes. Only by focussing on the three legs of the stool can any organisation hope to achieve the required alignment of organisation functions and regulatory understanding necessary to meet challenge and embrace the opportunities that Subject Access Requests represent.

CONCLUSION

Subject Access Requests are an important "canary in the coalmine" for an organisation because they shine a light on the strengths and weaknesses of your systems of processing for personal data and the governance functions that support them.

People submit Subject Access requests to a wide range of organisations for a wide range of reasons. However "because my lawyer made me do it" is not one of the main reasons, despite what some Data Controllers might want to believe.

The experience people have of submitting a subject access request, or even considering it, can affect their perception of the organisation they are dealing with. Overly legalistic, rigidly bureaucratic approaches damage the impression people have of your organisation. An engaged, 'customer focussed' approach allows you to develop a dialogue with the Data Subject, identify the underlying reasons (if any) for their Access Request, validate their identity, and verify the scope of data that they are looking for. To top it off, doing it that way increases the positive perception of your organisation.

Putting the Data Subject at the centre of the process, and ensuring you are meeting their Process outcomes and Information Outcomes means your organisation needs to consider how it is aligning Business, Information, and Technology across the organisation to ensure those outcomes are consistently delivered.

Currently organisations in Ireland, the UK, and Europe are bad at delivering on Subject Access Request outcomes. Up to 57% of access requests have a negative outcome for the Data Subject. Regulators are seeing a constant growth in the level of complaints about Subject Access request issues. The Irish Data Protection Commissioner reports that 53% of their complaints workload relates to Subject Access Requests.

The EU Data Protection Regulation will bring about fines of between €250,000 and €500,000 (or between 1% and 2% of global turnover) for a range of offences related to Data Subject Rights, including the Right of Access. Organisations that are failing under the current legislation face significant costs of non-compliance unless they act to improve their Data Protection capability.

Of course, improving your ability to quickly access and retrieve high quality data about data subjects that you can trust will have benefits to the organisation beyond just avoiding compliance penalties. Clever organisations will see beyond the fear and leverage Data Protection compliance and Subject Access Requests as a tool to drive better alignment of Business, Information, and Technology in their organisations.

Those organisations will need to develop holistic approaches that align Data Protection, Information Quality, and Information Governance to support the delivery of critical Data Subject Information Outcomes and Process Outcomes.

Castlebridge Associates can help.

ABOUT CASTLEBRIDGE ASSOCIATES

Castlebridge Associates is an Irish-based Information Management consultancy headquartered in County Wexford, with offices in Dublin. Castlebridge works with organisations to help them improve their internal capabilities to manage and govern information effectively.

Founded by an internationally respected expert in the fields of Information Governance, Information Quality, and Data Privacy, Castlebridge Associates works with a network of international partners to deliver high value-adding consulting and training services in the areas of Information Strategy and Architecture, Information Governance, Information Quality, and Data Protection and Privacy.

Our team are actively involved in developing the "best practice" standards and frameworks that organisations should be striving to implement. Our founder, Daragh O Brien, was a lead contributor on the IT-CMF's Enterprise Information Management capability, as well as contributing to the development of professional certifications in Information Quality Management, Data Protection, and Data Management.

We work with clients in a range of industry sectors including Public Sector, Transportation, Telecommunications, Financial Services, and Not-for-Profits. We also work with a range of innovative high potential start-ups advising on Data Governance, Privacy, and Information Architecture.

ABOUT DARAGH O BRIEN

Daragh O Brien, is an internationally regarded expert on Data Governance, Information Quality, and Data Protection practice. He is a Fellow of the Irish Computer Society, a member of the International Association of Privacy Professionals, a former Director of the International Association for Information and Data Quality (IAIDQ), and is currently Global Privacy Advisor to the Data Management Association (DAMA).

Daragh holds a degree in Business and Legal Studies from UCD, and is a Certified Information Quality Practitioner, Six Sigma Green Belt, and Certified Data Protection Professional. He lectures on Data Governance and Data Protection practice on the Law Society of Ireland's Professional Certificate in Data Protection Practice.

ABOUT DR. KATHERINE O'KEEFE

Dr. Katherine O'Keefe is an Analyst Consultant with Castlebridge Associates, specializing in Data Governance and Data Protection implementation and training.

Katherine has worked on Data Governance programme design for a leading telecoms company and for a leading airline and has worked with a number of clients on Data Protection compliance reviews and gap remediation.

CONTACT CASTLEBRIDGE


+353 76 6031850


enquiries@castlebridge.ie


Twitter.com/cbridgeinfo


https://www.linkedin.com/company/castlebridge-associates


https://www.facebook.com/CastlebridgeAssociates


Invent Centre, Dublin City University, Glasnevin, Dublin 9, Ireland