bsi.

...making excellence a habit.™

Responding to a Data Subject Access Request under the GDPR

A whitepaper

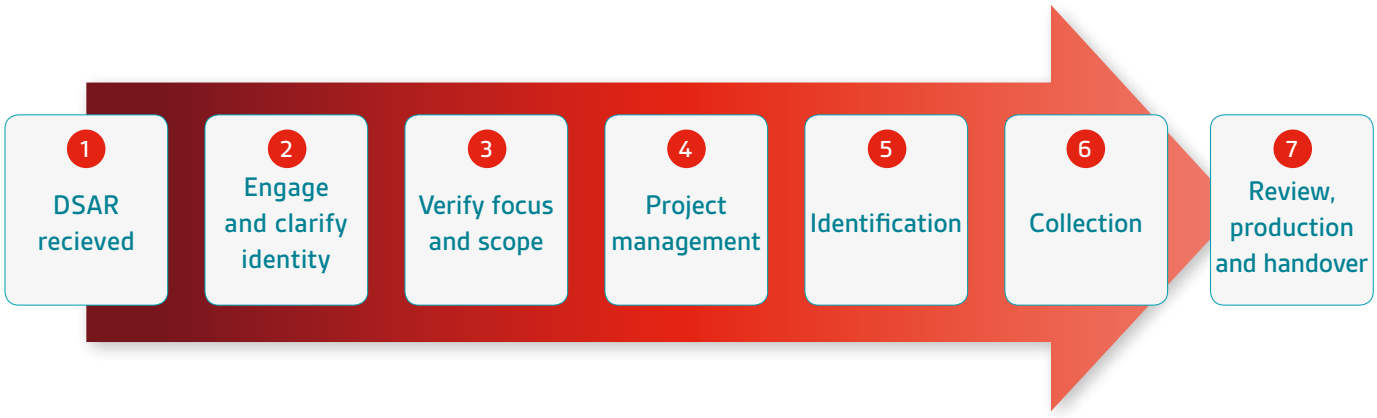
Introduction

This whitepaper discusses the challenges faced by organizations in complying with a Data Subject Access Request (DSAR) and the impact the General Data Protection Regulation (GDPR) will have in responding to such requests from 25th May 2018. This paper focuses on the typical workflows involved and includes recommendations and best practices. Information is also provided on some of the common pitfalls and problems encountered with the "aggressive requester".

From the 25th of May 2018 onwards, organizations that collect or process personal data of EU citizens will no longer have the deterring factor of charging a fee for responding to a DSAR. The GDPR has not only increased the rights of data subjects, but it has also greatly increased the awareness among the common person of their rights in this sphere. The GDPR is being introduced after all to increase transparency and awareness, and it has certainly been successful with this in the emergence of some rather interesting accounts of data subjects enforcing their rights to a copy of their personal data, amongst other rights. There is a concern that a trend may rise towards nuisance and disruptive DSARs being furnished on organizations by disgruntled ex-employees, persons with a gripe against the organization or the more daunting prospect of a person with enough knowledge to cripple an organization with an extensive DSAR. The motive behind these DSARs is not always clear but the end result for the organization may include a significant cost in responding, loss of time and opportunity cost, and a risk of a complaint to the relevant Data Protection Supervisory Authority should they fail to fulfil their obligations.

Preparation is key and a DSAR should not be a heavy burden for those organizations that are ready and aware of what steps must be taken to respond to such a request and what tools will assist them in doing so in an efficient manner.

This paper follows the typical workflow sequence in responding to a DSAR:



1 Receipt of a Data Subject Access Request

The GDPR opens up the possibility of a DSAR being levied on an organization through various means. A request need not be sent solely in writing over traditional mail or email channels; a request received verbally in person, verbally over the phone, or even via social media channels may now be considered valid requests.

As such, staff will need a minimum level of awareness and training to be alert and mindful of their obligations around the receipt of these requests.

The source of the request could potentially be an important indicator of the purpose or motive behind the request and often places a requester into the following groups:

- a privacy focussed person with a general interest in how their data is being handled
- a disgruntled ex-employee
- a client or customer who has been irritated or
- an opportunistic requester with the intent of causing some mischief

For an ex-employee, the request may come in through the HR department or a line manager. For the other categories of requesters, the request would usually come in directly to the designated Data Protection Officer (DPO). However, it may also be received through other channels including IT, Compliance, Operations, or through more unconventional means such as hand dropped letters to the front desk. There is also the possibility of requesters sending in requests through a live chat portal if this is a resource offered on the website of the recipient organization.

2 Engage with the requester and clarify their identity

So, you have recognized and received a DSAR. The next step is to go through a structured process of responding to the requester.

The organization should proceed to verify the identity of the requester to ensure they are dealing with the correct person and prevent a potential security breach. Requesting a copy of the requesters ID is good practice here along with a copy of a utility bill to verify their address.

Organizations should also be mindful that the collection of this verification data is a further collection and processing of the requesting data subject's data. A retention period for this data should be considered and incorporated into the process and communicated to the requester.

At the same time that the identity of the requester is being verified, the DPO or other designated person should make a decision on whether the request is valid or not and provide acknowledgment of this to the requester.

In making the decision to accept or refuse a request, the DPO or other designated person should consider some of the following points to identify whether the request is valid and if it must be responded to:

- Does it specifically relate to Personal Data?
- Is the person entitled to the data?
- Are they requesting work related data or data that constitutes Intellectual Property of the organization?
- Is the request manifestly unfounded or excessive?
- Is the request seeking a copy of data which could be deemed excessive based on the background circumstances of the request such as backup tapes, log files, phone recordings or other uncommon sources?

The DPO should also be clear and transparent on the timelines involved in responding to the request and make clear when the clock starts ticking. If the organization considers that the period to respond commences when it receives the identification and any additional information sought this should be made clear to the requester. The time between receipt of the initiating request and the receipt of identification and any further information requested may be a number of days so this communication is important to set expectations.

3 Verify the focus and scope of the request

The DPO or other designated person may request further information which is reasonably required in order to assist in identifying and finding the personal data sought in the DSAR. The following are some of the items which may form part of responding to a DSAR, and may be specifically requested in some circumstances:

Internal DSAR: Ex-Employees	
Requested Items	**Some Considerations**
Full HR file	Are all of the contents of the HR file considered personal data?
All emails the requester sent or received	Are these all personal? Is there an Acceptable Usage Policy where employees are required to use emails for business purposes only? Can your search distinguish between work related emails and internal emails? Are there chains of emails containing both work related and personal data such as emails sent to line managers and HR.
Any emails by others mentioning their name	What is the scope of these? Line managers to other management/HR?
Any meeting minutes with their names mentioned	Are these work product and intellectual property of the company or personal data?
Any documents they were signatories on	Are these work product and intellectual property of the company or personal data such as contract of employments versus contracts they signed for the benefit of the company?
Any other documents they are mentioned in	Are these work product and intellectual property of the company or personal data?
Any documents they produced	Are these work product and intellectual property of the company or personal data?
Swipe card data for physical access	Is this readily available? Does it require assistance of a 3rd Party provider?
CCTV data	Is this readily available? Does it require assistance of a 3rd Party provider? Is there a specific time period of interest or could it be potentially considered as a broad and excessive request? Who else features in the CCTV which may need redacting?
Phone recordings	Is this readily available? Does it require assistance of a 3rd Party provider? Is there a specific time period of interest or could it be considered as a broad and excessive request?

External DSAR: Privacy Focussed Citizens; Irritated Clients; or Opportunistic Requesters	
Requested Items	**Some Considerations**
Full copy of data held on systems	Is the organization planning to rely on structured data sources only when complying with such a general request? If so, it should be communicated to the requester.
A list of specific and targeted sources and which may include • All unstructured data • Backup data • Log data • CCTV data • Phone call data • Web chat log data • Reception desk sign in logs • CRM records • Order history • Emails or CRM records where the DSAR itself has been mentioned • Any other specific sources	This type of request may stem from a more opportunistic or aggressive requester. Be wary of these types of requests and the communication around what you commit to handover in this scenario.

Irrespective of the source of the request, it is good practice to communicate with the requester and seek reasonable clarification around the focus and scope of the request where it is required. It would be good practice to follow up with a clear structured list of data sources and parameters in which the organization will pursue in complying with the DSAR. Where the focus and scope of the request can be reduced with agreement of the requester, it may save significant time, effort and costs in responding to the request.

An aggressive and opportunistic type requester should be treated with an extra degree of caution and organizations should ensure they are clear in the scope of the request, set expectations for both parties on what will form part of the reasonable and proportionate response to the request. There may be opportunities to push back on "excessive" items within a request and it is worth mentioning that an organization could consider charging an administrative "reasonable fee" for a request post May 2018 when a request is manifestly unfounded, excessive or repetitive. However, the application of this exemption and fee needs to be monitored until guidance is issued from the Article 29 Working Party/ European Data Protection Board (EDPB), or from individual Supervisory Authorities.

4 Project management

It is recommended to have a project management mind-set when responding to a DSAR. The project management approach should be initiated once a request is received. The importance of following a structured approach and delineating responsibility will become more important as the project progresses through the next phases. A DSAR encompasses all the main project management processes including:

Scope	Identify and agree on the scope and focus of the request from the start with the requester and the agreed timeline.
Change	Change must be controlled. Further Personal Data may be identified as the project progresses at each of the subsequent stages.
Planning	Planning is essential and a clear delineation of responsibilities is important. The timeline for each stage should be documented.
Management	Management of the team, objectives and coordination between the stakeholders as each stage is important
Success	Success is measured on the satisfaction of the delivered DSAR, the quality of it, and the number of records identified, reviewed, and redacted within the timeframe.
Monitoring	Monitoring and controlling risk is important

The DPO is the natural project manager of a DSAR and will learn from training and experience of the best strategies to employ and what areas present the biggest risk to the deliverable timeframe.

5 Identification

The success of the identification stage will depend on the culture of information governance within the organization and the quality of the GDPR readiness campaign undertaken.

The focus and scope verified with the requester should be assessed against the organization's Detailed Processing Records (as required by Article 30 of the GDPR). Identifying the data in structured and unstructured data sources in line with the agreed scope is important for a successful response.

An eDiscovery/information management type data mapping exercise is useful to help identify the following sources against the data flow diagrams and personal data inventory which can include the following:

Electronic Structured Sources (Databases; CRM systems); Electronic Unstructured Sources (Shared drives); Email Sources; Cloud Environments (SharePoint, Office 365 etc.); Hardcopy Data within Scope; What departments and/or personnel have control of these sources; What custodians may have data within scope (mailboxes of managers etc.); Any 3rd party providers required to assist (processors of CRM databases etc.); Logs; Backup Tapes; CCTV; Phone Recordings; and the volume of potential data for collection from each source.

6 Collection

The collection stage can present some challenges depending on the scope of the request and the processes in place. It will encompass gathering all of the potential sources within scope into one central repository.

A clearly defined workflow process should be in place where each person/department with responsibility for the collection exercise has a clear set of guidelines to follow. The IT department will play a significant role in the collection exercise but they will need cooperation from the other relevant business units. Information management and eDiscovery experts may be required to provide expert guidance on the pertinent actions, decisions, and to validate the integrity of the data collected and assist in the subsequent review, production and handover phases.

It is important to agree at the outset whether search criteria will be applied at the collection stage and this should be communicated and agreed with all stakeholders in advance. All steps and decisions made should be documented as they may be required in the event that the completeness of the delivered DSAR is queried by the requester. The search criteria could include: Date ranges; Names; Addresses; DOB; Email addresses (work and/or personal); Phone numbers; PPS/NI; Passport number; IP addresses; Drivers licence number; Biometric data identifiers; Work ID number; Job position; Salary; Login names; Nicknames; and any other personally identifiable information.

7 Review, production and handover

Once the data is collected in a central repository, arguably the most time consuming and challenging part of responding to a DSAR begins. Below is a non-exhaustive list of the questions which will need to be addressed during the review and handover stages, depending on the number of requests and volume/type of data in scope:

- **Who is responsible for reviewing the data for the request?**
  - Does the review team have an adequate level of training in the privacy domain?
  - Are they aware of the background and scope of the request?
- **What system or tools, if any, are being used to review the documents or track the review progress and categorization of data?**
  - Is there a de-duplication facility?
- **Who will:**
  - Oversee the review?
  - Batch and organize documents between reviewers?
  - Oversee control quality and sampling for consistency?
  - Make final decisions on contentious documents and redactions?
  - Is there a possibility that privileged or commercially sensitive documents should be withheld and will a log of these be retained?
  - Is legal oversight and sign off required?
- **What is the volume of documents/records to be reviewed? Does this include attachments?**
  - How many records can a person review per day?
  - Based on the volume of records and human review speeds, are there any tools available to help speed up the review process and overcome potential inefficiencies in the workflow?

Continues >>

- **How will additional personal data items discovered during the review be handled?**
  - Will an iterative cycle of identification and collection be employed where such personal data items are discovered during the review stage (e.g. an additional personal email address of the data subject)?
- **Has redaction time been factored into the time line as this will take significantly longer to undertake?**
  - Extensive redactions may be required where the consent from other data subjects contained in the documents cannot be achieved.
  - Will software be used to complete redactions? (An un-redacted document with another individual's personal data disclosed as part of the handover will be considered a data breach.)
  - Will a log of redaction reasons be maintained?
- **How will difficult documents/sources such as Microsoft Excel documents (with hidden cells and tabs), CCTV or phone recordings be handled and how will they be redacted?**
- **What format will the finalized data be handed over in?**
  - hardcopy or electronic?
  - Native files may show additional hidden metadata such as last modified and last saved by which may be an inadvertent disclosure?
  - Is additional time required to convert the data into another format such as PDF?
  - How will the data be securely transferred? Will the data be encrypted?
- **How long will the handed over data be retained for?**

The review of the data has many moving parts and requires careful thought and consideration. This area has the highest risk of running over the allocated time and budget if not kept under control and adequately planned. Having a streamlined process in place which is efficient and can take advantage of technological solutions will help meet deadlines.

There are a number of additional anomalies which can occur in responding to a DSAR and contingency should be built into your response planning in the event a request is received at an inconvenient time such as in the build up to or over the Christmas period. It should also be considered whether there is a need for legal assistance or support from a third party that specializes in this area.

Summary

The GDPR will arrive on the 25th May 2018 and bring with it a host of changes. While there is currently a lot of discussion around the potential fines in the region of up to €20 million or 4% of annual turnover, it is important that organizations do not overlook some of the primary rights of Data Subjects which could have a significant impact on an organization. The number of Data Subject rights which can be levied on an organization could cause significant costs and administrative burdens on the organization. Having a structured plan in place and considering whether additional technology is required to support the plan will reduce the risk of non-compliance in responding to DSARs.

BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services

Security awareness

Phishing and user awareness training, online solutions, social engineering and simulation testing

Information management and privacy

Information risk management, privacy, data protection, eDiscovery and forensics

Compliance and testing

PCI DSS services, Cyber Lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

Find out more

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com

bsi.