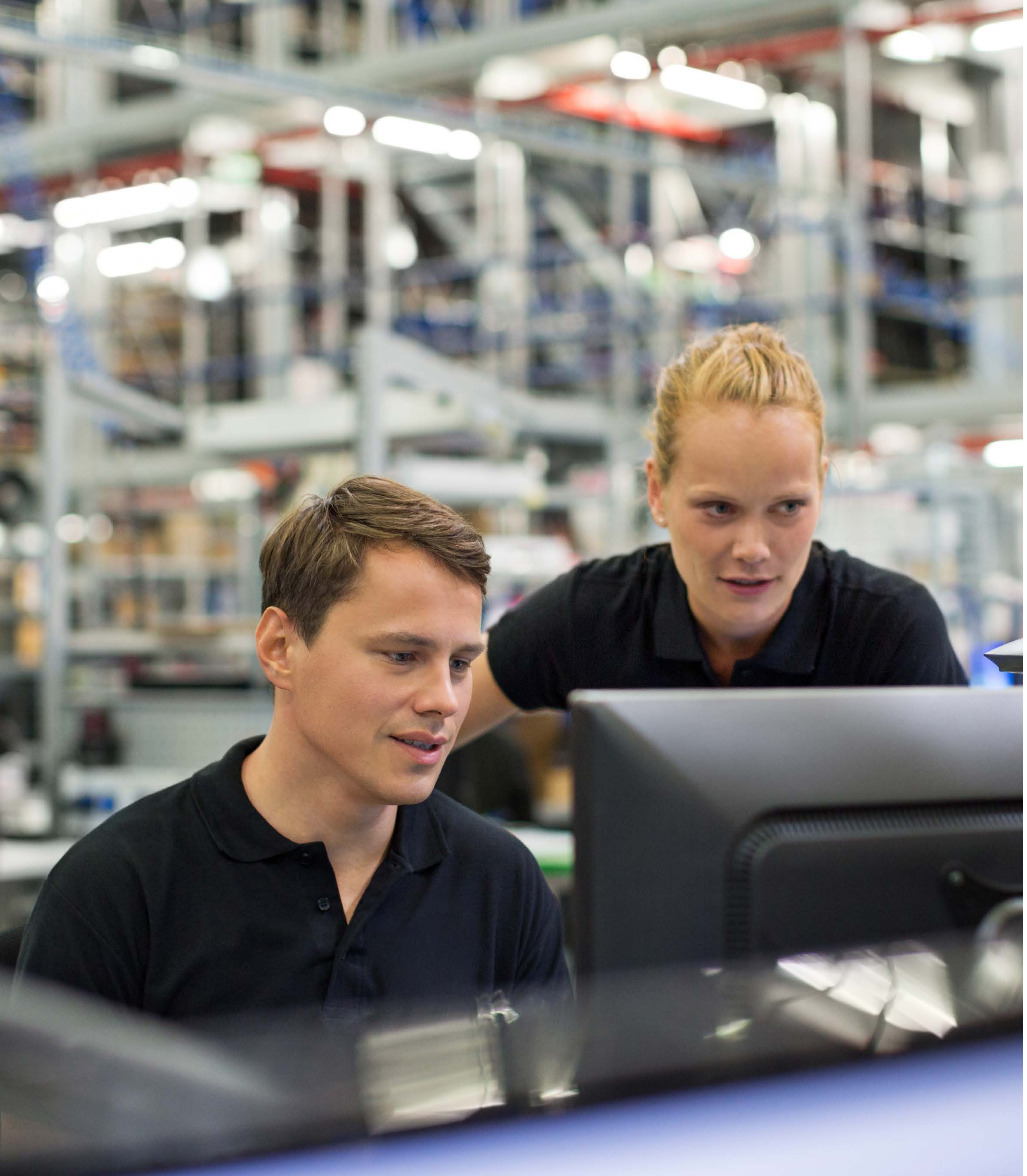
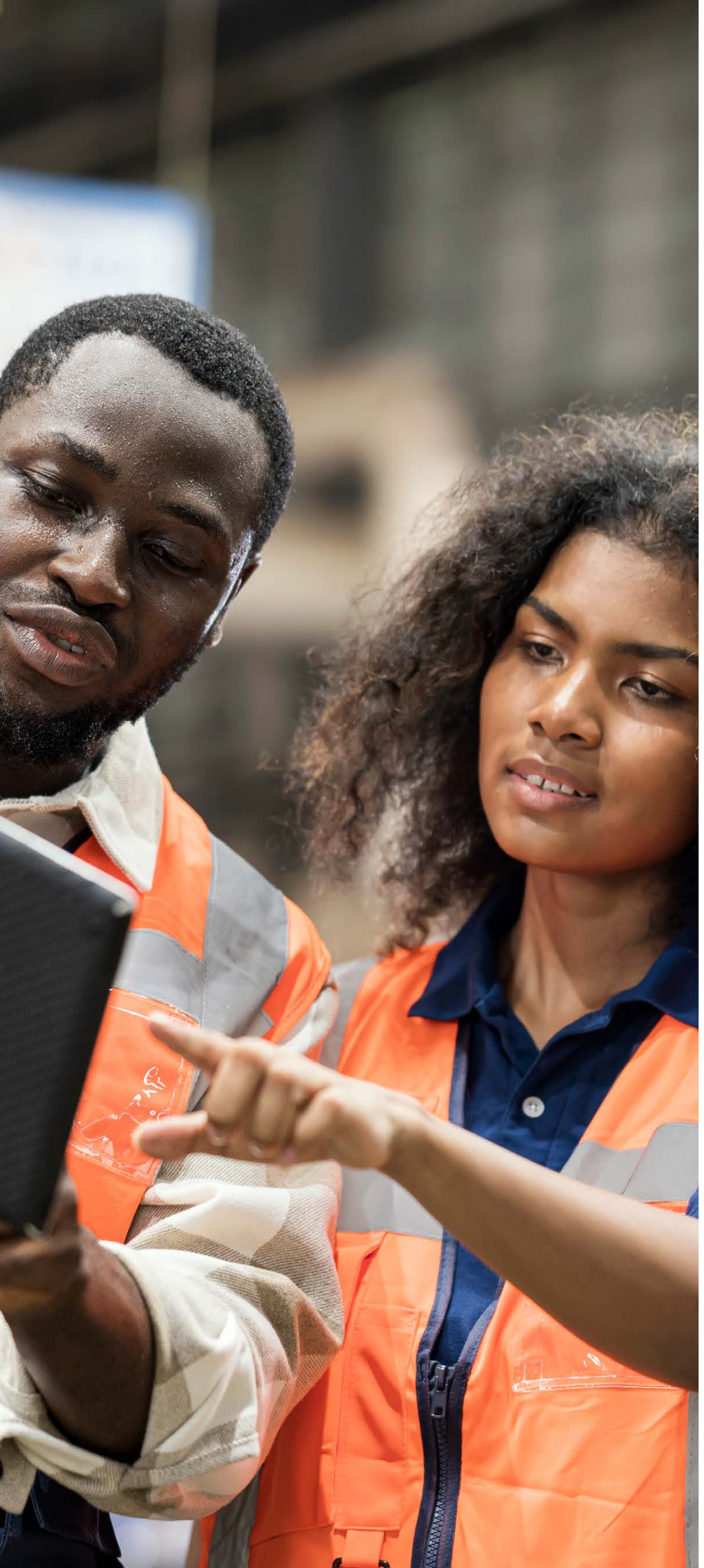
Challenges organizations face ensuring compliance with Data Subject Access Requests (DSARs)

BSI white paper



Contents



Introduction

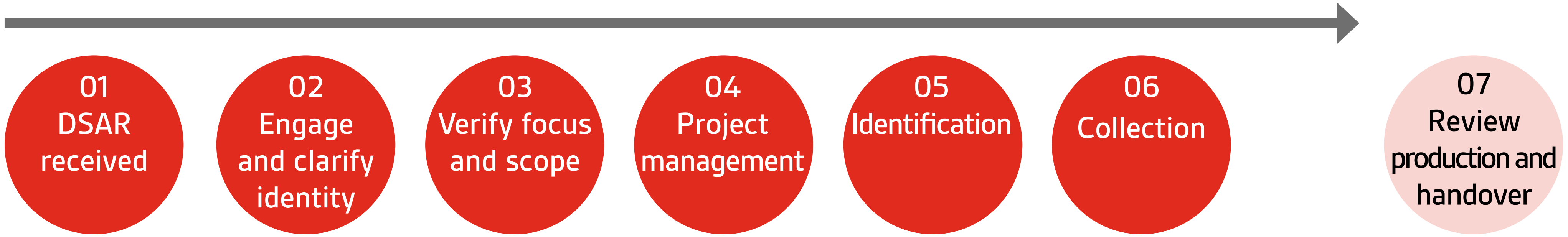
In this insights paper, we discuss the challenges that organizations face when ensuring compliance with Data Subject Access Requests (DSAR). We explore the impact that the EU and UK General Data Protection Regulations (GDPRs) have had in responding to such requests, for almost 5 years. We also focus on the typical workflows involved and include recommendations and what would now be considered best practices.

Since 2018, all organizations that have collected or processed personal data of EU and UK citizens no longer had the right to charge a fee for responding to a Data Subject Access Request (DSAR).

GDPRs have increased the rights of data subjects, but they have also increased the awareness amongst data subjects of their rights to their data.

The GDPRs were introduced to increase transparency and awareness, and it has certainly been successful. We have seen the emergence of some fascinating accounts of data subjects enforcing their rights to a copy of their personal data, amongst other rights. The early concerns about a trend towards nuisance and disruptive DSARs being submitted to organizations by disgruntled former employees have occasionally come to fruition.

Being prepared for receiving a DSAR is essential, even if the organization only processes very little personal data. It's just as essential to know how best to respond to a DSAR. A DSAR is a straightforward request to comply with for the organizations who are 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.



01 DSAR received

02 Engage and clarify identity

03 Verify focus and scope

04 Project management

05 Identification

06 Collection

07 Review production and handover

Staff continues to need a minimum level of awareness and training to be alert and mindful of their obligations around the receipt of these requests.

01 Receipt of a data subject access request

The GDPR's opened up the possibility of a DSAR being levied on an organization through numerous means; however the European Data Protection Board (EDPB) produced some guidance that states, "It should be noted that the controller is not obliged to act on a request sent to a random or incorrect email (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights".[1]

Staff continues to need a minimum level of awareness and training to be alert and mindful of their obligations around the receipt of these requests. Providing staff with only awareness is **NOT** enough. Training is required on the specifics of how the organization manages DSARs internally.

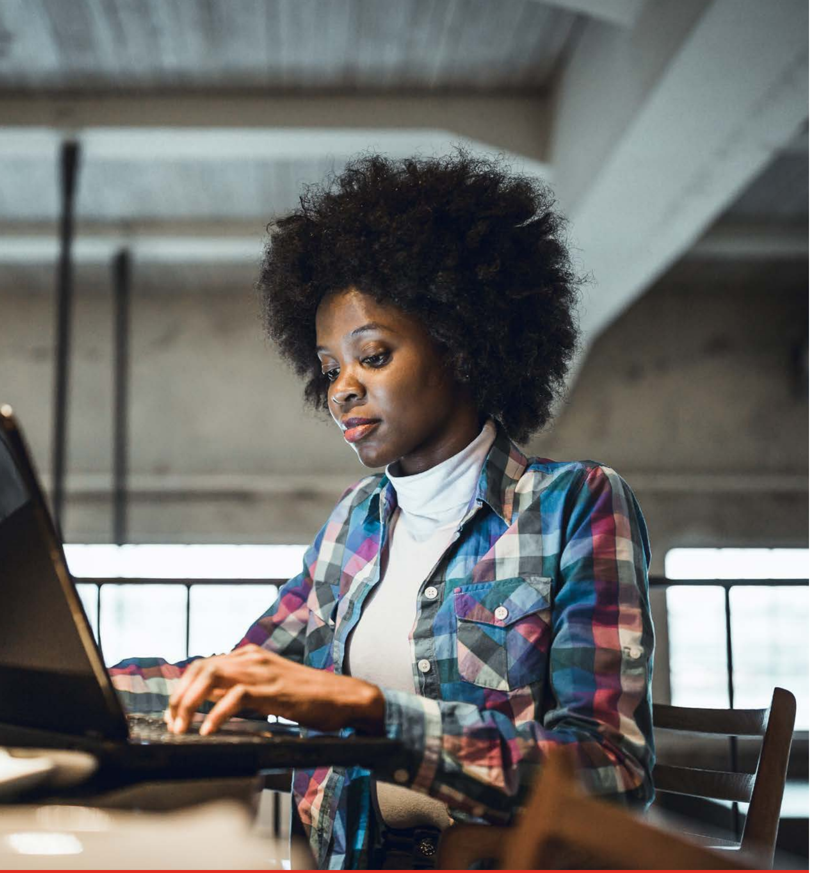
The source of the request may be an indicator of the purpose or motive behind it and often places a requester into the following groups:

- A privacy-focused person with a general interest in how their data is being handled
- A disgruntled former employee
- A client or customer who has been irritated or
- An opportunistic requester with malicious intent.

For a former employee, these requests typically come in through the HR department or from their former line manager. For the other categories of requesters, the request would usually come in directly to the nominated Data Protection Officer (DPO).

However, it may also be received through other channels including IT, Compliance, and Operations, or through more unconventional means such as hand-dropped letters to the front desk

[1] Page 21, Section 53 – European Data Protection Guidelines – https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf – Accessed on 20/12/22



The DPO should offer advice clearly and with transparency on the timelines involved in responding to the request

02 Engage with the requester & clarify their identity

It is recommended that the organization proceed to verify the identity of the requester to ensure they are dealing with the correct person and prevent a potential security breach. The EDPB guidelines clearly state: "as a rule, the controller cannot request more personal data than is necessary to enable this identification, and that the use of such information should be strictly limited to fulfilling the data subjects' request."

Requesting copies of even more personal data, to allow data subjects to confirm that they are whom they claim to be could be considered a breach of the data minimization principle within Article 6 (1)(c). As a potential digital channel of communication may already exist between the data subject and the organization, it would be considered a good, safe data protection practice to authenticate the data subject by confirming previous messages or by another method.

Using utility bills or any other means should be considered an absolute last resort, ONLY if the organization can prove it 'reasonable doubt' as to the identity of the data subject. Passport data shouldn't be used to confirm identity, as this type of data is commonly used in identity theft and may become compromised if a data breach occurs within an organization. This will lead to a much higher risk to the data subject and greater risk to the organization from any regulatory action taken.

Whilst this process may seem the opposite of the organizations' current methodology of confirming identity, it is considered best practice and follows the EDPB guidelines, plus is in keeping with overall GDPR compliance.

The rationale for this is that organizations must be mindful that the collection of any verification data is also classed as a further collection. It is also strictly for the purpose of processing the requesting data subject's data. Any other use of this data may constitute a breach of Article 6 (1)(b). A retention period for this data MUST be incorporated into the process and communicated to the requester. It has to be recorded within the Record of Processing Activities, where required under Article 30 of the GDPRs.

At the same time that the identity of the requester is being verified, the DPO should offer advice to the organization, as to allow them to make a decision on whether the request is valid or not and provide acknowledgment of this to the requester. Remembering that the DPO's role in the organization is advisory in nature.

The advice given by the DPO, as to the decision to accept or refuse a request, 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 constitute Intellectual Property of the organization?
- Is the request manifestly unfounded or excessive?

The DPO should offer advice clearly and with transparency on the timelines involved in responding to the request, and the organization should be left in no doubt 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 (again as a last resort) and any further information requested may be a number of days, so this communication is important to set expectations.

[1] Page 21, Section 53 – European Data Protection Guidelines – https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf – Accessed on 20/12/22

03 Verify the focus and scope of the request

The DPO should advise the organization on what may be requested in terms of further information 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 could be specifically requested in some circumstances:

Internal DSAR: Former 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 products and intellectual property of the company or personal data?
Any documents they were signatories on	• Are these work products and intellectual property of the company or personal data such as contracts of employment 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 the assistance of a 3rd Party provider?
CCTV data	• Is this readily available? Does it require the assistance of a 3rd Party provider? • Is there a specific time period of interest or could it be potentially considered a broad and excessive request? • Who else features in the CCTV which may need redacting?
Phone recordings	• Is this readily available? Does it require the 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
A 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 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. • Remember, it is not for the organization to scrutinize the motive of the requester. The organization must compliantly fulfill the request.

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 is recommended to follow up with a clearly structured list of data sources and parameters which the organization will pursue in complying with the DSAR. Where the focus and scope of the request can be reduced with the 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 it is recommended that organizations ensure that they are clear in the scope of the request and set expectations for both parties on what will form part of the reasonable and proportionate response to the request.

There may be opportunities to question 'excessive' items within a request and it is worth remembering that an organization could consider charging an administrative "reasonable fee" for a request, **ONLY** when a request is manifestly unfounded, excessive, or repetitive. However, the application of this exemption and fee needs to be monitored under the guidance of the European Data Protection Board (EDPB), or from individual Supervisory Authorities. Before charging a reasonable fee based on Article 12(5) of the GDPR, 'controllers should provide an indication of their plan to do so to the data subjects'. The latter has to be enabled to decide whether they will withdraw the request to avoid being charged.

04 Project management

It is recommended to have a project management mindset 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 may appear to be the natural project manager of a DSAR; however, it is the organization’s responsibility to respond, **NOT** the DPO. The DPO can advise the organization based on the training they provide and experience of the best strategies to employ and what areas present the biggest risk to the deliverable timeframe.

05 Identification of personal data

The success of the identification stage will depend on the culture of information governance within the organization and the maturity/ quality of the ongoing GDPR compliance program. 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:

- Electronic Structured Sources (Databases; CRM systems)
- Electronic Unstructured Sources (OneDrive, GoogleDrive)
- Email Sources; Cloud Environments (SharePoint, Box, 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.

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.

06 Collection

The collection stage presents some of the greatest challenges depending on the scope of the request and the processes in place. It encompasses gathering all the potential sources within the scope into one central repository.

A clearly defined workflow process should be in a place where each person or department with responsibility for the collection exercise has a clear set of guidelines to follow. The IT department plays a significant role in the collection exercise, however, the IT department does need a lot of 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 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 upon 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; National Insurance number (UK); Passport number; IP addresses; Drivers license detail; Biometric data identifiers; Work ID number; Job position; Salary; Login names and any other personally identifiable information.

07 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 adequate 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?

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 timeline as this will take significantly longer to undertake?

- Extensive redactions may be required where consent from other data subjects contained in the documents cannot be achieved.
- Will the software be used to complete redactions? (An unredacted 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 which may be an inadvertent disclosure.
- Is the 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 an efficient, efficient, streamlined process that 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.

As an organization, it is your responsibility to look after individuals' data and when data subjects make this request, it is their right to do so.

Summary

To date, there have been almost 1,400 fines imposed by the Supervisory Authorities across the EU and UK, of which the general term of 'insufficient fulfillment of data subjects rights', has proven to have been the case in almost 10% of these. The fines have resulted in over €2 billion having to be paid by organizations globally, which is in the scope of the GDPRs. It remains important that organizations do not overlook some of the primary rights of Data Subjects which could significantly impact an organization.

The number of Data Subject rights that can be levied on an organization could cause significant costs and administrative burdens on the organization, however, this can be mitigated by having a structured plan in place and considering if additional technology is required to support the plan will reduce the risk of non-compliance in responding to DSARs.

It is worth remembering the importance that as an organization, it is your responsibility to look after individuals' data and when data subjects make this request, it is their right to do so.

Why BSI?

An independent body like BSI can provide a wide range of data protection expertise, assistance in scoping, data mapping, recommended approaches and the use of market-leading technology to tackle the challenges presented by a DSAR. We help reduce the amount of data to review and provide you with a defensible approach.

Learn more

Our legal, compliance, and technology experts become an extension of your team and deliver best-in-class technology to empower your organization to create efficient and defensible data management workflows into managed services in conjunction with leading-edge, innovative technology alliance partners – **all to inspire trust in a more resilient world where we can resist threats.**

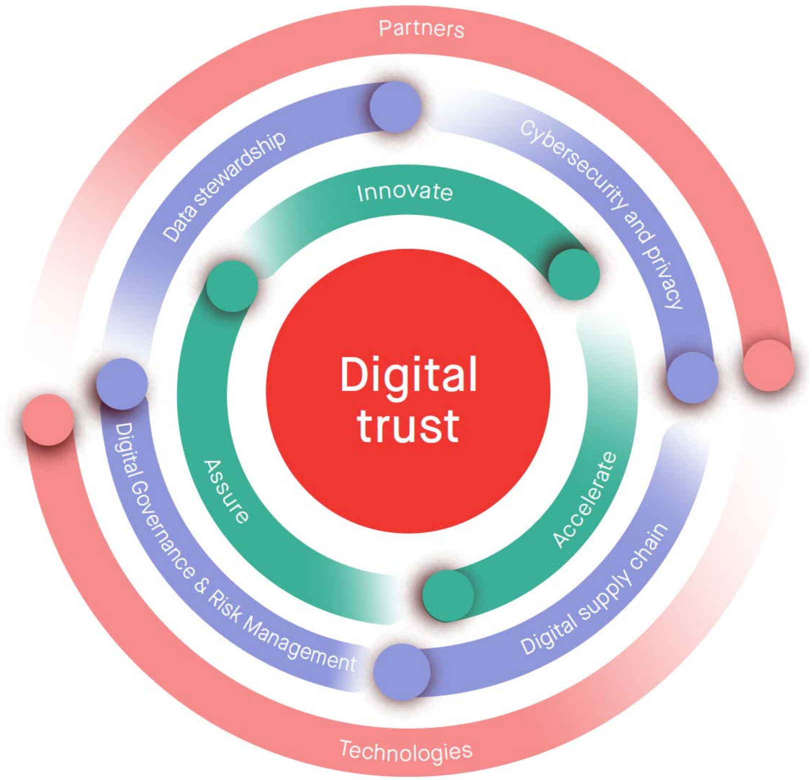
About BSI Digital trust

At BSI Digital trust, our global expertise enables our clients to better enhance their cyber resilience, protecting their critical information and IT infrastructure, people, and brand reputation.

We support organizations through our integrated portfolio of services including providing digital and cyber risk advisory, security testing services to clients, as well as looking at areas like data privacy, compliance and governance, as well as niche capabilities such as e-discovery and e-forensics.

Digital trust aggregates four subdomains with interlocking strategies, plans, and actions:

1. Cybersecurity and privacy
2. IT Governance and risk appetite
3. Data stewardship and AI ethics
4. Digital supply chain



> **“Digital trust is the confidence users have in the ability of people, technology and processes to create a secure digital world.”**
>
> Mark Brown, Global Managing Director, Digital Trust Consulting Services, BSI

Get in touch

EMEA
Call: +353 1 210 1711
Email: digitaltrust.consulting.ie@bsigroup.com
Visit: bsigroup.com/digital-trust-ie

UK
+44 345 222 1711
digitaltrust.consulting@bsigroup.com
bsigroup.com/digital-trust-uk

US
+1 800 862 4977
digitaltrust.consulting.us@bsigroup.com
bsigroup.com/digital-trust-us

Follow us on

Disclaimer
BSI is an accredited Certification Body for Management System Certification and Product certification. No BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 year period following completion of consultancy.