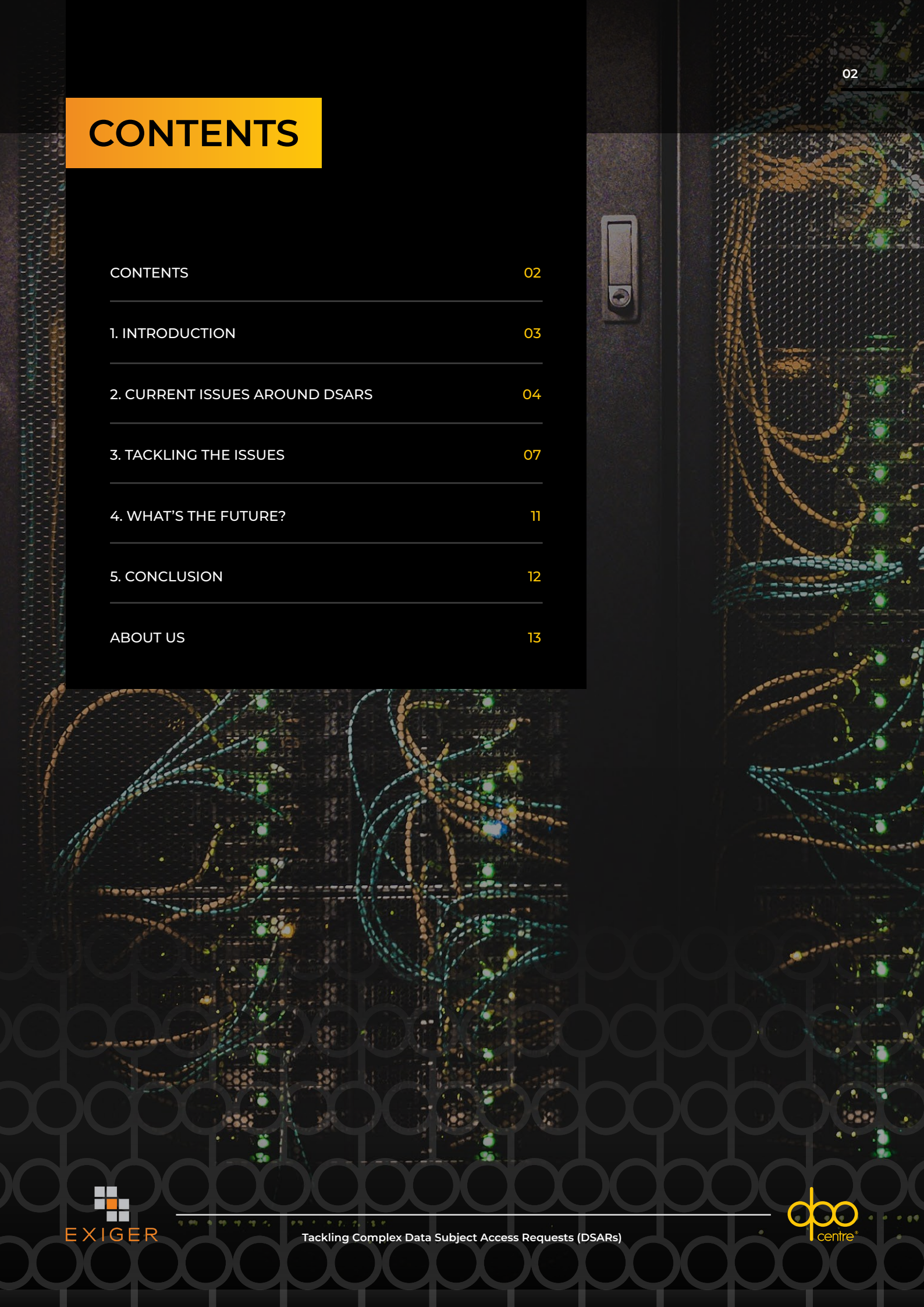
TACKLING COMPLEX DATA SUBJECT ACCESS REQUESTS *(DSARs)*

EXIGER | Intelligence

dpo centre®

CONTENTS



1. INTRODUCTION

The implementation of data protection legislation, such as the General Data Protection Regulation ('GDPR'), the Data Protection Act 2018 and California Consumer Privacy Act (CCPA) has brought with it a significant number of individuals ('Data Subjects') invoking their rights permitted by these laws. Whilst other data information rights laws and statutory provisions (such as the Freedom of Information Act 2000) give individuals limited access to information, the GDPR extends the right of access to personal data further than anything seen previously. It is important that such requests are handled fairly and within the strict timeframes permitted, whilst ensuring that the application of these rights does not undermine other data protection obligations on your organisation, such as preserving the privacy rights of other 3rd parties and adhering to any duties of confidentiality.

Data Subject Access Requests (DSARs) can be complex by their nature. It is not uncommon for professionals, including data protection professionals, to have a variety of different views on how to approach DSARs (such as when redactions need to be applied). Dealing with them can therefore be rather time-consuming and resource heavy. In November 2020, the DPO Centre commissioned research into consumers' views on how companies handle their personal data. The research revealed that whilst only 1 in 10 respondents had considered submitting a DSAR, 44% believed that companies were mishandling their personal data. This research shows that there is considerable scope for the number of DSARs that companies receive to increase significantly, and it is thought that "Companies should expect DSAR requests to increase over the coming years as one of the fallouts from the pandemic." It is likely that the government rolling back its furlough scheme will trigger a wave of redundancies in all sectors, which could act as a catalyst for significant numbers of DSARs as employees seek to find out the basis for their employers' decisions.[1]

You can begin to see DSARs as a potential starting point to a number of litigations and class actions. The mandated fulfilment times and risks associated with wrongful disclosure of personal data pose increasing challenges to organisations, increasing costs and drawing resources away from their frontline products and/or services. Hence, when responding to DSARs, organisations need to have processes in place which are sustainable and adaptable for larger cases.

Bringing together the expertise of two leading companies in data protection compliance, this white paper discusses several challenges that can make responding to DSARs particularly difficult, along with how they can be dealt with. The solutions to dealing with these challenges are two-fold. First, the procedures and practices that companies can embed within their data processing operations to make responding to complex DSARs more manageable. Second, the technology/tools that help to facilitate and gain efficiencies on these procedures. By implementing the correct procedures and having the appropriate tools, companies can greatly reduce the burden and risk of having to deal with DSARs, saving them both time and money.

2. CURRENT ISSUES AROUND DSARS

There are several factors which may increase the difficulties for companies dealing with DSARs that need considering when creating a DSAR response procedure.

2.1 LARGE VOLUMES OF PERSONAL DATA

Collating data as part of a DSAR can often be challenging due to the number of documents and data assets involved. Whilst you may hold very little personal data on some Data Subjects (e.g., if an individual has merely enquired about opening a bank account), for others you may hold vast amounts of data going back many years (such as for an employee, or an aggrieved individual in the middle of a dispute with your organisation). Given that personal data may be located in several different databases across different departments, and be held in multiple formats, locating and collating the relevant documents is time-consuming and resource heavy.

In most corporate houses, employees use email as their main form of communication. Over 300 billion emails were sent and received each day in 2020. That number is expected to increase to 361.6 billion by 2024. Considering that in responding to a DSAR all this information must be reviewed and potentially redacted, it is unsurprising that the estimated cost to a company of fulfilling a DSAR runs into the thousands of pounds. Manual review of documents may no longer be practical, and in the case of an increasing number of organisations, simply not feasible. To comply with regulations, the organisation must leverage technology to cull the data that is out of scope and only produce information relevant to the specific data subject.

2.2 PROCESSING AND REVIEWING COMPLEX DATA TYPES

Just as there may be large volumes of personal data to be provided, the data is likely to be spread across multiple locations and be held in varying formats within numerous systems. There may also be a large volume of paper based records which require detailed searching and compiling strategies.

While some electronic data may be compiled within a structured CRM or CMS database, and therefore fairly straightforward to retrieve, evolving technologies and new electronic communication platforms are being implemented at a rapid pace, and these present new challenges to organisations. It is critical to know what data each communication system holds and how the data is stored. Depending on the new technology that these eComms platforms (chat/ email/ audio) are built on, corporate IT will need specific skills and knowledge to forensically extract the relevant subject's data should the need arise.

It should be noted that non-text data such as audio recordings, or CCTV video images may also need to be retrieved and included within a DSAR response. Non-text data can be more challenging to process as there are fewer automatic search functions. Finally, there may also be personal data stored in non-electronic format, requiring manual retrieval.

2. CURRENT ISSUES AROUND DSARS CONT...

2.3 IDENTIFYING PERSONAL DATA OF OTHER PEOPLE

In many cases, documents that relate to the Data Subject's request will also include the personal data of other individuals, such as staff members who have dealt with the Data Subject, the Data Subject's family members, or individuals who have made allegations against the Data Subject. The presence of a third party's personal data within the information to be disclosed complicates responding to DSARs in two ways.

First, searches must be conducted to identify if any third party personal data is present. This is made especially difficult if personal data is likely to reference multiple third-parties. Secondly, once personal data of other people is identified, decisions must be made over whether to disclose or redact (i.e., obscure) the information in question. While there are ways to automatically identify addresses/phone numbers/credit card details and other similar information, it is more challenging to identify the presence of other terms by which someone can be identified. For example, simply calling someone a 'glasses wearer' is enough to identify them if they are the only person who wears glasses in that office. Additionally, with internet slang and texting abbreviations accelerating the rate of the change in communication styles, there are new terms that are constantly being added to our vocabulary that can also identify an individual.

2.4 REVIEW AND REDACTION OF TEXT AND NON-TEXT DATA

Oftentimes, there will be cases where the provision of personal data may conflict with other data protection or privacy rights, or potentially prejudice other legal provisions or interests (e.g., where the personal data of a third party is contained within the documents, or the information is confidential or privileged). Therefore, once the documents that fall within the parameters of the DSAR have been retrieved, they need to be reviewed to ensure that they are able to be disclosed. There may be several considerations to be taken into account and it may be difficult to determine which should take precedence. Once a decision has been made as to whether to disclose information or not, you will need to undertake an exercise in redacting any information you do not want to disclose. Whilst redacting text data is more straightforward, although time consuming, redacting non-text data is far more challenging, often requiring technical expertise and the creation of detailed rationales for such redactions.

2. CURRENT ISSUES AROUND DSARS CONT...

2.5 HANDLING PRIVILEGED INFORMATION AND ITS DISCLOSURE

Like with the personal data of third parties, there may be confidential or privileged information included within the files retrieved as part of a DSAR. On one hand, disclosing confidential or privileged information to an individual who does not have authorisation to access it has legal implications. On the other, failing to disclose information to a Data Subject based upon the mistaken idea that it is confidential may give rise to grounds for a complaint or legal challenge. Therefore, it is important that accurate judgements are made about the disclosure of information. This presents challenges for companies because it may be difficult to identify which documents are confidential – just because something is marked 'confidential' does not mean that it is. Furthermore, judgements must then be made as to whether there is any overriding interest that means it should be disclosed.

Although DSARs can be challenging for companies to deal with for many different reasons, it should be remembered that, in most circumstances, they must be complied with within one month of receiving the request. Whilst the GDPR does allow for this time frame to be extended on a month-by-month basis for up to two further months, this is only permitted where the request is complex, or the individual has made a number of requests. In this context, "complex" means the complexity of the request itself, not how difficult it would be for the organisation to provide the data. Therefore, it is vital that you have the appropriate policies and procedures in place to enable the one-month deadline to be met.

3. TACKLING THE ISSUES

For any organisation, it is critical to know where their customers' and employees' data resides. The first priority is to have an up to date data map for the entire organisation or business unit. The data map should be reviewed and audited at regular periodic intervals. Also, any new software or products used by these departments that may contain personal data should be registered on a central database and revisited annually for an audit. Many software solutions already exist to index data that reside within a particular system. This allows organisations to search what personal data they may have held for any Data Subject. Furthermore, technology consulting firms should be used to forensically extract the data if the corporate IT team has any doubts at any point.

3.1 LARGE VOLUMES OF PERSONAL DATA

You can reduce the volume of personal data that you hold on Data Subjects by ensuring that you have an appropriate retention policy in place that determines how long different types of personal data are kept. Some retention periods are determined by law, but others you can determine within your company. Choosing retention periods requires careful consideration as you must be able to justify your choice and ensure that you are not keeping it for longer than needed, as per the GDPR's Storage Limitation principle. It should be noted that once a retention policy is in place, there must then be the mechanisms in place to ensure that it is followed.

It may also be useful to review what personal data you collect from individuals and consider whether all of the data you process is necessary to fulfil the specified purpose for which it was collected. For example, it may be necessary to ask for an individual's national insurance number when they open a bank account, but not when they make an initial inquiry. Only capturing the personal data you require for a specified purpose relates to the principle of Data Minimisation. Adhering to this principle should help to reduce the volume of personal data you hold on individuals and therefore help to make DSARs more manageable.

Whilst the above practices will help prepare for future DSARs, at the time of receiving a request you can ask the Data Subject to specify the information or processing activities that their request relates to. Whilst it is not permissible to require the requestor to narrow the scope of their request, you can ask them to provide some additional details to help you respond effectively and locate the personal data that they are seeking. For example, you could ask them to provide the likely dates within which the processing may have occurred, or the name of any members of staff with whom they have engaged. Asking the right questions on receipt of a request may save you a significant amount of effort down the line, whilst also helping the Data Subject get exactly the information they are looking for.

From a technology perspective, expanding datasets are not the only challenge; the rate at which the data is expanding is also a critical factor that an organisation needs to take into account. Leveraging high-speed processing power and use of advanced analytics is not a luxury, but rather an essential. Organisations should use analytic techniques to cull down the redundant data held. Examples of these techniques could include de-duplication of data or communication threading analysis, both of which help to reduce the volume of the unique copy and inclusive contents of an email thread.

3. TACKLING THE ISSUES CONT...

3.2 PROCESSING AND REVIEWING COMPLEX DATA TYPES

Similar to dealing with large volumes of data, it is often helpful to work with the Data Subject to determine which types of data they want access to, thus limiting the scope of the search required. Further to that, targeted searches need to be conducted across each database to locate and retrieve all the specified information. It is therefore essential that you have a clear idea of where various datasets are held and how to access them. As such, carrying out a data discovery exercise may be helpful. Depending on your data processing activities and the complexity of data flows within your organisation, you may want to seek advice on how to accurately map your data.

As personal data consists of more than just an individual's name, multiple different search terms or criteria must be used to filter through the various databases to ensure that all relevant personal data is found (e.g., the individual's name; customer ID number; email address etc). This process can be made much easier with a robust records management regime in place that ensures data is stored in a logical manner and logged accurately.

Using document characteristics and analytics techniques to group a similar nature of data together can help to drive up efficiency by finding different types of items that you may wish to exclude from review and disclosure. For example:

- Using document characteristics to search for all emails considered 'newsletters'
- Identifying all mass emails by searching by recipient count (e.g., all emails with 20 recipients or more)
- Identifying any privileged content using privilege search terms or using analytics and reviewing them in clusters

It is important to note that there is no guarantee that all documents found using these methods will all be excluded from disclosure. However, it will help to significantly speed up the review process. Technology Assisted Review (TAR) can also help to manage and support review of large and complex cases leveraging the power of machine learning.

3. TACKLING THE ISSUES CONT...

3.3 IDENTIFYING PERSONAL DATA OF OTHER PEOPLE

Searching for any personal data belonging to third parties within the documents to be disclosed in a DSAR requires knowledge of what the law considers to be personal data. Pieces of information that may initially seem insignificant may make an individual identifiable. Therefore, you must ensure that you are searching correctly through the documents. In many cases, it may be clear which third parties' personal data will be included within the information. For example, if the Data Subject has a shared bank account with their partner, their partner's name is likely to appear in the collated documents. However, things become more complicated when the identity of possible third parties mentioned within the documents is unknown.

Considering this on a case to case basis is time consuming. In today's era of Artificial Intelligence (AI) and machine learning, AI-enabled e-Discovery technologies are being further leveraged to not only automate the process of personal data identification and streamline the DSAR process, but also to automatically redact that information effectively and efficiently, saving both time and money. This is achieved by using search terms as a repository whereby terms refer to characteristics of a person. For example, terms of all race, religions and discrimination words. Pattern recognition creates a regular expression to match a specific pattern within an organisation, such as employee number, branch code etc., as this information can identify a person. Coupled with Artificial Intelligence, such as entity recognition, data enrichment and modelling, it can power Natural Language Processing (NLP) and play a key role in identifying personal data.

3.4 REVIEW AND REDACTION OF TEXT AND NON-TEXT DATA

Where there is a conflict between fulfilling a DSAR and other data protection or privacy rights, or other legal provisions or interests, a balance must be struck between the competing factors. When considering whether to disclose information that may identify a third party, for example, you must weigh up the requestor's right of access, with the data protection, privacy, and any other rights of the third party. In some cases, it may be appropriate to ask the third party to consent to the disclosure, however, where that is not appropriate a test of reasonableness must be undertaken. This requires a careful balancing assessment that may require expert guidance due to the many factors to be considered, including whether the third party is cited in their personal or professional capacity, the nature of the information, and the potential harms that may arise from disclosure.

The technology for auto redaction on both text and non-text data is available. The key is to ensure non-disclosure of other personal information or privileged content by discovering and redacting them. An appropriate quality assurance workflow, that could still require an element of manual review, needs to be employed to verify the documents prior to disclosure. The aim is to create a repeatable and auditable process along with the automation. The key is to strike the right balance between automation, manual quality control and advisory support from a subject matter expert.

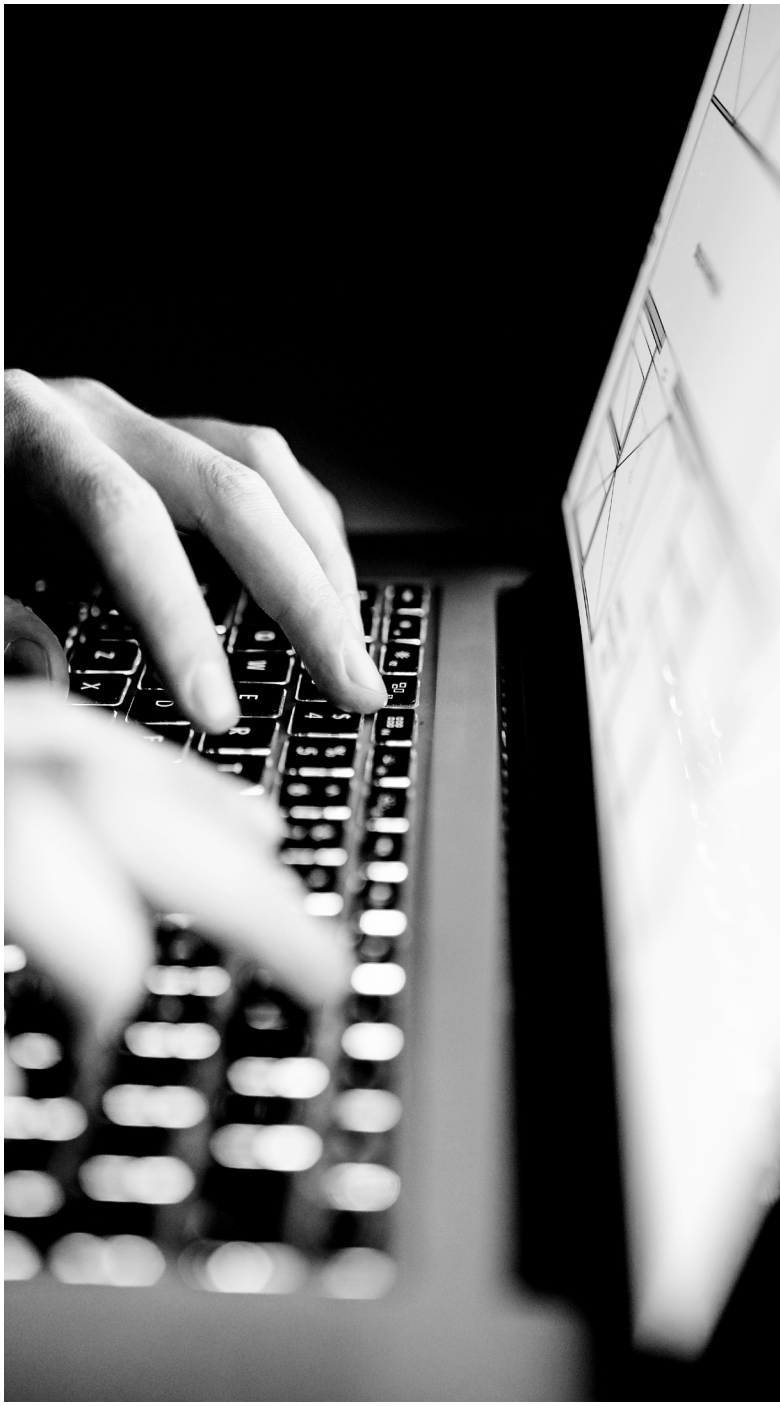
3. TACKLING THE ISSUES CONT...

3.5 HANDLING PRIVILEGED INFORMATION AND ITS DISCLOSURE

Determining the confidentiality of information involves detailed consideration of a range of factors of which context is paramount. As such, confidentiality must be determined on a case-by-case basis and thus requires thorough examination. To be deemed confidential, the information must have a quality of confidence about it and the relationship between the parties giving and receiving the information must impart a duty of confidence. Although in some cases this may be fairly obvious, for example, information covered by a non-disclosure agreement is confidential, there are many other cases which are less so.

Employing appropriate Workflow using eDiscovery technology can help to identify potential privileged contents by using predefined privileged terms or using a predefined privileged model to bring back documents which are likely to be of a privileged nature. This technology can be employed in two stages. First, to identify potential privileged documents early-on and group them together to speed up the review process. Second, to be used as an additional quality control layer to ensure that any documents to be disclosed to the Data Subject do not contain any privileged information.

Once information has been deemed confidential, it cannot be disclosed unless there is an overriding public interest in its disclosure. This again demands a case-by-case assessment which will require a reasonable amount of expertise in this area. Whatever decision you make with regard to both the confidentiality of information and its disclosure, it is very important to document your decisions and the rationale behind them. This is so that, in the event an individual or supervisory authority challenges you, you have justifications recorded to refer back to.



4. WHAT'S THE FUTURE?

As Brexit has pushed the discussion over 'adequacy' into the limelight, and with data breaches and court cases against the world's largest companies continuing to hit the headlines, data protection is opening up to wider audiences. The general public are becoming far more aware of data protection and privacy and, resultantly, their associated rights. The COVID-19 pandemic and the accompanying move to remote working has served to further propel data protection to the forefront of public consciousness. This is a change that is unlikely to reverse in the coming years, given the ever-increasing shift 'online'.

With most employees working remotely, this is likely to spike up the data volume within communication systems even higher. Communications on chat platforms have already seen a significant rise and this trend is set to continue.

With the lockdowns and various travel bans, the global economy is enduring a tough time. The resulting economic uncertainty has both micro and macro level effects on every organisation and even in society. Concern around job losses is predicted across various industry sectors, and there is a strong chance of rising volumes of DSARs from employees as measures are introduced by organisations looking to emerge and survive in the post-COVID economy. If handled incorrectly, there is a possibility of litigation or potential class actions which could spin off from these small DSARs.

The predicted increase in DSARs will have significant economic impacts for companies on the receiving end. Research conducted by Guardum in 2020 calculated the average cost of fulfilling a DSAR to be £4,884.53. For companies with over 5000 employees this rose to £6,812.13. Moreover, the average number of working hours spent responding to requests was 83, increasing to 136 for companies with over 5000 employees.[2]

These numbers demonstrate that DSARs could begin to take up increasing amounts of both monetary and human resources, so companies need to have the appropriate systems in place to ensure requests are dealt with efficiently. Diligent organisations should act now and start setting up appropriate processes and procedures before risking being overwhelmed in the face of complex or multiple DSARs.

5. CONCLUSION

It is clear that DSARs present multiple and varying challenges for companies and dealing with them can be onerous. Having robust procedures and practices in place within your organisation, both for dealing with DSARs but also for processing personal data more generally, will greatly aid in responding to any requests received and reduce the significant burden that they can impose. There are many technologies that are available in today's market within the DSAR management process. Selecting the right technology and harnessing it for appropriate use is vital. No single technology can solve every DSAR challenge. It is important to find the right balance between technology automation and leveraging subject matter expertise when developing organisational procedures to effectively deal with requests.

Implementing these procedures in the most efficient way will often require both data protection expertise and sector specific knowledge, therefore in many cases it will be necessary to seek expert advice to ensure GDPR-compliant practices are implemented in a way that is not detrimental to your organisation's commercial goals.

ABOUT US

ABOUT EXIGER

Exiger is the global authority on financial crime and fraud, revolutionising the way corporations, banks and governments manage risk through its combination of practical expertise, award-winning technology and process excellence. In recognition of the growing volume and complexity of data and regulation, Exiger is committed to creating a more sustainable compliance environment through its holistic and innovative approach to problem solving. Powered by DDIQ and Insight 3PM, Exiger takes an analytics-led, technology-enabled approach to everything we do. Exiger has worked with a number of organisations to successfully build a technology enabled end-to-end DSAR workflow solution, saving both time and money while meeting regulatory obligations in a repeatable and predictable manner. This solution has significantly improved the predictability with which clients can respond to requests, reduced the level of effort required by staff by 75%-80%, and significantly lowered the associated costs. Exiger operates out of 11 offices with more than 500 employees around the world.

Learn more at exiger.com.

ABOUT THE DPO CENTRE

The DPO Centre is a specialist data protection and compliance consultancy, providing data protection related services to over 600 clients from a wide variety of sectors, ranging from commercial, financial services, tech, health, education, and 3rd sector organisations.

Formed in July 2017, the DPO Centre has a large team of permanently employed Data Protection Officers (DPOs) located throughout the UK. Every member of this team is an experienced DPO who is knowledgeable and highly adaptable, so can deliver the exact level of support required and in the precise manner you require it.

The DPO Centre can assist with one-off projects, such as data protection audits, dealing with DSARs and conducting DPIAs. The DPO Centre also provides ongoing support and guidance as your designated DPO, taking ownership of the day-to-day responsibility for the role, or as your EU or UK Representative required under Article 27 of the GDPR. DPO services are provided on a 'fractional' basis, so based on the exact level of resource required to meet your evolving needs.

The DPO Centre is based in London and Dublin and has a network of offices across Europe.

CO- AUTHORS:
Avigyan Das – Associate Managing Director - LinkedIn
adas@exiger.com
Jariya Laoriendee – Director - LinkedIn
jlaoriendee@exiger.com

Lenitha Bishop – Head of DPOs at The DPO Centre - LinkedIn
Ben Seretny – Data Protection Officer - LinkedIn
hello@dpocentre.com

(1) Research commissioned by the DPO Centre and conducted by Opinium Research, 13-17 November 2020 based on a 2,000 nationally representative weighted sample.

(2) Guardum, 'Guardum DPOs: DSARs and the impact of COVID-19' (May 2020). Research conducted by Sapio Research, April and May 2020 based on a sample of 100 UK DSAR managers working within companies with 250+ employees. Report presentation can be found here.

www.dpocentre.com
+44 (0) 203 797 1289
hello@dpocentre.com
Join us on LinkedIn

London
The DPO Centre Ltd
50 Liverpool Street
London
EC2M 7PR United Kingdom

Exiger
32nd Floor,
25 Canada Square
Canary Wharf
London E14 5LQ

EXIGER

dpo centre