aiimi

DATA. DIGITAL. INSIGHT. | DSARS

MANAGING DSARs.

ARE YOU ADOPTING THE RIGHT APPROACH?

NOT ALL DSARS ARE MADE EQUAL

UNSTRUCTURED DATA ⊠

3RD PARTY DATA ⊠

SENSITIVE IP ⊠

DISPARATE SOURCES ⊠

UNSTRUCTURED DATA ⊠

WWW.AIIMI.COM

AS YOUR BUSINESS EXPANDS, SO TOO DOES THE VOLUME – AND COMPLEXITY – OF YOUR SUBJECT ACCESS REQUESTS (SARS, OFTEN ALSO KNOWN AS DSARS – WHERE THE 'D' REFERS TO DATA). WITH SARS/DSARS RISING YEAR ON YEAR, CAN BUSINESSES MANAGE THEIRS MANUALLY, OR DOES AN ABUNDANCE OF DATA DEMAND INTELLIGENT DISCOVERY AND AUTOMATION?

With GDPR rules now long cemented in British and European law, more of your customers are familiarising themselves with their data rights, principles and options. This includes accessing the data a business holds on them, as well as exercising their GDPR right to be forgotten (RTBF) – deleting any personal information held where it is no longer required. With the volume of your business data growing, and the number of Data Subject Access Requests rising, personal data is fast becoming a needle in an ever-expanding haystack.

For smaller businesses, or those early into their corporate journey, DSARs can be strenuous, but simple enough to manage with a basic search solution. If the volume of your monthly requests is low, and your data is stored in a handful of easily accessed structured data stores, you may find that your DSARs remain quite manageable. Yet as time moves on, or as your business evolves, the demand for DSARs can soon outweigh capacity; and as your data subjects' profiles elaborate, so too does the complexity of their requests, heavying the load on your HR, IT and Legal teams.

THE DIFFICULTIES OF DSAR MANAGEMENT

As with any task, DSARs become more fraught as your volume of personal data grows; and with more data points come more chances for inadvertent data leaks, more complex requests, and longer DSAR completion times. Over time, businesses will need to adopt deeper, wider and more targeted DSAR retrieval to retrieve every piece of relevant personal data and – more critically – adhere to stringent data protection rules. This year,

the Information Commissioner's Office shared in a **press release** that it had received 15,848 complaints relating to DSARs between April 2022 and March 2023; a significant number, no doubt collative with the 60% of respondents who reported a rise in DSARs, as seen in an **EY Law survey** over a similar period.

For context, consider the multiple chains of data that might make up the database of a financial institution. Their existing data tools may be sufficient for case management or prescribed workflows, and be able to handle typical day-to-day tasks. However, over the years, a single data subject will contribute escalating volumes of data.

> DISPARATE DATA TOOLS AND SOURCES, SPREAD BETWEEN SEVERAL DEPARTMENTS INCLUDING HR, LEGAL AND IT, WILL HAVE AN INCREASINGLY FRACTURED DATA THREAD, MAKING IT HARDER TO CONTEXTUALISE THEIR SUBJECTS' DATA JOURNEY.

As data on the individual evolves, there is also heightened risk that third parties will exist among their data; beneficiaries or Powers of Attorney, whose sensitive data is at risk of being revealed or overlooked for deletion. With the hierarchy of data deepening, the task of contextualising, connecting and classifying this data becomes more strenuous. All of which raises a pertinent question: once your DSARs become more than a simple search can provide, how can you be confident that you've managed to find all the data you need to disclose or – in the case of RTBF requests - delete?

DATA DISCOVERY TOOLS

As these complicated questions mount, so too does the need for more specialist **data discovery tools**. Providing more extensive insight into your data subjects using secure AI and machine learning, these solutions deliver a full data narrative of any data subject across your company's every data point, locating and identifying relevant files and key data fields and identifying potential third-party information that could be at risk. This way your subject, and any related sensitive information, is automatically identified by their interconnected data.

Essentially, while a basic search can find text matches, a Data Discovery Tool finds answers. Still, not all DSARs are made equal – and whether a data discovery tool is relevant for your business depends on the nature of your requests.

IF YOU FIND YOURSELF IN NEED OF ANY OF THE BELOW EXAMPLES, IT MIGHT BE TIME TO INVESTIGATE YOUR OPTIONS....

_01

UNSTRUCTURED DATA DISCOVERY

Some of your subject data will be stored within a recognised database format, often designated by identifiable fields or line entries. But your wealth of unstructured data is a little less binary; existing in its raw format – as media files or office documents, for example – this data lives outside established databases and provides a richer level of detail. It's useful, but it's not immediately compatible with the established data formats, meaning you could be missing out on some key contextual evidence. A data discovery tool underpinned by AI can intelligently scour your unstructured data, identify fields that fit into more structured data formats, and present these findings in a more holistic context.

YOU CAN'T
PROTECT DATA
YOU CAN'T SEE

_02

A COMPLETE DATA PICTURE

Sometimes, finding disparate data still doesn't provide the full picture. While less specialist solutions can help find your most obvious data points, they can't always identify related or supporting data – that detail that leaves gaps in your subjects' data narratives. A data discovery tool takes your data search beyond the basics, looking within a file to ensure all relevant personal data is discoverable, and any potentially related data is identified. Because advanced data discovery tools harness AI to continually find and enrich data, this in-depth data view is available every time you kick off a discovery search. The result is a full body of evidence, spanning your entire data mesh.

_03

REDACTIONS TO PROTECT THIRD PARTY DATA

In industries such as healthcare – where a single patient can be linked to other GPs, dependants, pharmacists or surgeons – it can be easy to overlook third parties that exist within your subject's records. Using AI, a data discovery tool adopts data enrichment processes, such as pattern matching and Named Entity Recognition, to identify fields such as NI Numbers, names, addresses and emails, redacting them at the user's discretion and enabling stricter adherence to data protection laws. Crucially, this is an automatic process, with all kinds of personal data identified without the need for user input, nor having to conduct a specific search. The benefits here are both proactive and reactive; your DSAR is handled diligently and dutifully, while any sensitive data discovered through an always-on data classification process can be automatically given the appropriate security labels and risk scores, helping you keep data safe.

_04

ENTERPRISE SCALING

Your business runs on hundreds of data sources and multiple software solutions, each creating or processing their own structured and unstructured data. These might be specialist solutions, such as HR or accounting software, invaluable for their operational efficiency. However, their siloed nature often means they don't share collaborative capabilities with your other tools and solutions, creating data disparity across your departments. A data discovery tool can act as a unifier, connecting these disparate applications into one common solution. This helps to deliver a full data picture while ensuring all data stays within its designated apps and access rights.

_05

UNITY BETWEEN TEAMS

As sensitive information piles up, the burden of your Data Access Governance becomes heavier. Knowing how to identify sensitive info, classify it and ensure it is seen only by the appropriate handlers is itself a major challenge. A data discovery tool can distinguish specific data types and provide the administrative tools to put access rights only in the hands of those who need it. In doing so, you don't only respond to your access requests but proactively manage your current and future data risks, including protected and regulated data such as your corporate IP or department specific documents. This delegation doesn't have to be divisive; where data is shared between teams, it can be made available from within your data discovery tool and discoverable across all departments – accurately, consistently and completely.

> OFTEN, SPECIALIST SYSTEMS AND SOURCES ARE SILOED AND CAN'T COLLABORATE; THE RESULT IS DATA DISPARITY ACROSS YOUR DEPARTMENTS. A DATA DISCOVERY TOOL CAN ACT AS A UNIFIER, CONNECTING THESE DISPARATE APPLICATIONS TO DELIVER YOUR ENTIRE DATA PICTURE.

01
ADAPTIVE
AI

ADAPTIVE AI

Discovers, identifies and compiles personal data without the need for manual searches, providing a full data picture for a single data subject.

02
SMART
REDACTION
SUGGESTIONS

SMART REDACTION SUGGESTIONS

Finds hidden sensitive data and recommends deletions for complete, compliant peace of mind and more diligent regulatory adherence in future requests.

03
SENSITIVE
DATA
DILIGENCE

SENSITIVE DATA DILIGENCE

Identifies classified or restricted data, suggests appropriate classifications, and allows full Data Access Governance for users and teams.

04
UNSTRUCTURED
DATA
SUPPORT

UNSTRUCTURED DATA SUPPORT

Enables collaboration and discoverability among your structured and unstructured data, allowing for greater data visibility, clearer context and a more complete data picture.

IS IT TIME TO INVEST IN DATA DISCOVERY FOR DSAR MANAGEMENT?

The benefits of data discovery tools are clear, but some businesses will find more suitable use cases than others. Before deciding for yourself, consider the volume of your DSARs, your wider data governance needs, and the difficulties of managing each – there may be more proportionate solutions available.

01

SIMPLE REQUESTS.

MAY BE MORE SUITED TO A **MANUAL WORKFLOW**.

A team of approximately 2–3 delegated staff in a single department (e.g. legal, or HR), managing mainly structured sources and low volumes of DSARs, all within manageable timeframes. These may be practicable with manual ROPA and checklists, while still adhering easily to ICO regulations.

← SIMPLE REQUESTS.

02

STANDARD REQUESTS.

AN **AUTOMATED WORKFLOW** MIGHT BE MORE APPROPRIATE.

A team of data handlers, managing multiple data subjects and types across 2 or more databases. They may be able to identify crucial or sensitive data efficiently, but want to speed up response times and lessen the risk of errors. They may be finding it harder to work to ICO standards and timeframes.

← STANDARD REQUESTS.

03

COMPLEX REQUESTS.

WOULD BENEFIT MOST FROM **AI-POWERED DATA DISCOVERY**.

Rapidly expanding businesses with more complex requests, higher volumes of unstructured data, disparate data sources and risk of third party data exposure. They may work in larger industries, have a broader database of clients and third parties, or have data with a long 'shelf-life' that evolves consistently.

← COMPLEX REQUESTS.
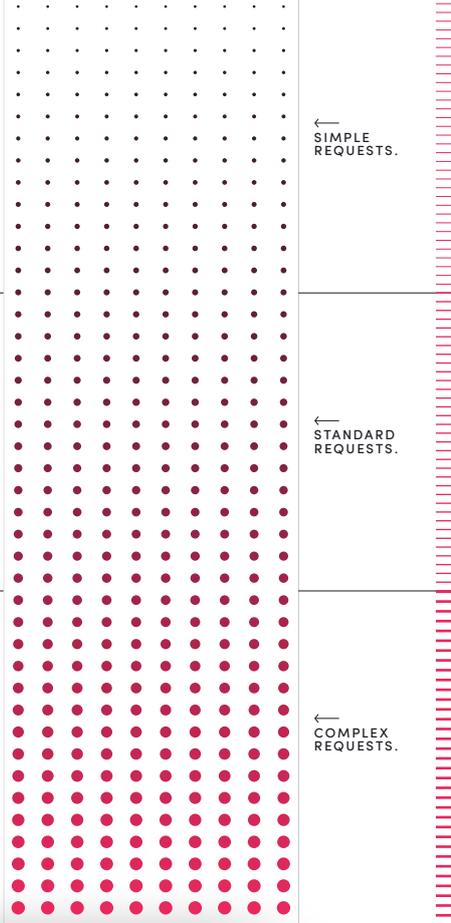
THE PATH TO DSAR DILIGENCE

Remember that a data discovery tool is not designed to merely automate DSARs. Instead, think of it as an enabler: a way to encourage data proficiency among users and departments, while delivering the full data picture across an entire business.

With DSARs written into business and GDPR law, the only certainty is their continued growth. For businesses whose data capabilities are struggling under limited capacity, a proactive approach ensures their every request is readily prepared, contextualised, and accounted for.

DATA.
DIGITAL.
INSIGHT.

aiimi

WE
TO ———— CONNECT ———— PEOPLE
INSIGHT