Picture credit: AdobeStock

LIFE OF PII

Michael Downs *reveals why data discovery remains fundamental despite Data Use and Access Act reforms*

Personal data has become one of the most valuable assets modern organisations can hold. From customer profiles and financial details to employee data and healthcare records, personally identifiable information (PII) plays an important role in how businesses function, operate, compete and grow. Personal data empowers personalisation, informs strategic decision-making and underpins effective service delivery. And the amount of it available to businesses has grown exponentially in more recent years.

According to IBM, 2.5-quintillion (18 zeros) bytes of data is now created daily, with 90 percent of the world's data having been created in the last two years alone. For organisations, keeping a grip on increasingly expansive data landscapes is a challenge. IBM also reveals that unstructured datasets comprise 90 percent of all enterprise-generated data – information that's housed in everything from documents to emails, contracts, images and collaborative content. Additionally, much of this data is duplicated, incomplete or even obsolete, which only adds to the difficulties that firms face when it comes to data governance.

Looking ahead, things are only set to become more difficult. It's forecast that global data generation will again triple between 2025 and 2029. For organisations, it's therefore critical to implement effective data management practices sooner rather than later.

While data itself is becoming increasingly difficult to manage, it's simultaneously coming under increasing fire from nefarious actors. Research from Microsoft shows that cybercriminals are attempting to steal data in more than 80 percent of attacks and that over half of cyberattacks with known motives were driven by extortion or ransomware. Whether intentionally as a result of these active threats, or mistakenly through data mismanagement, it's estimated that millions – if not billions – of people have already had some of their personal data leaked, with nearly 58-billion data points exposed since 2004. It is against this backdrop that an ever-stronger spotlight is being shone on the data management protection practices of organisations globally.

It's forecast that global data generation will triple again between 2025 and 2029

GDPR was introduced with the aim of giving individuals greater control over their personal data and to legally require organisations to handle that data responsibly, transparently and securely. In order to be compliant, firms must know exactly what sensitive and PII they hold, how it is stored, how it is used and how it moves across various systems and networks.

One important consumer right that falls under GDPR is Data Subject Access Requests (DSARs), enabling individuals to see which of their personal data is held by an organisation. However, the Information Commissioner's Office (ICO) revealed that the failure of organisations to meet DSARs formed a significant proportion of the 42,315 data protection complaints it received in its latest report. It's a concerning reality. One that suggests that many organisations are continuing to scramble to locate, collate and provide individuals with their personal data, which may well be scattered and archived in unstructured forms across cloud and on-prem environments.

This cannot be the norm. GDPR has been put in place for a reason – personal data is highly valuable and can become a major threat if it lands in the wrong hands. According to the Global Anti-Scam Alliance (GASA), scammers stole an estimated £9.4-billion from UK consumers over the past 12 months.

For organisations, there's also significant risks. Not only can GDPR breaches lead to fines of up to 4 percent of annual turnover, but firms may also suffer from irreparable reputational damages. One survey found that almost a third of consumers would stop doing business with a company known to have compromised cybersecurity.

This is not to say that aligning with GDPR is straightforward. Take DSARs – while requests from customers contacting ecommerce sites might simply involve names, email addresses, physical addresses, phone numbers and purchasing history, DSARs submitted by former employees can be much more complex. The latter can involve data spanning years of correspondence and projects.

On top of this, organisations have become increasingly cautious of DSARs. Indeed, cybercriminals may use these requests to obtain personal data surreptitiously. It is in the face of these hurdles that the Data Use and Access Act (DUAA) received Royal Assent last year, introducing measures designed to alleviate the burdens faced by companies when it comes to DSARs. Specifically, firms have been alleviated from conducting exhaustive searches that can be incredibly time consuming, with the DUAA having aligned with ICO guidance on: "reasonable and proportionate" DSARs. Additionally, the new legislation allows firms to pause DSARs until entities are verified and extend deadlines for complicated requests.

In every sense, the DUAA has helped to make it easier for firms to comply with the DSARs aspect of GDPR. However, it does not lessen the fundamental need for organisations to ensure they know exactly what data they hold, where that data resides, how it is used and how it is managed.

The new legislation serves as the perfect wake up call. Compliance has become easier to achieve and so firms have never had a better time to ensure that they are aligned with GDPR, and properly managing sensitive data and PII.

Effective data management starts with visibility. The question for many within this context will centre around where exactly to begin. How can companies regain full control of their data and implement effective data management practices that enable them to properly track, classify and protect sensitive and personal data, even as the data landscape continues to become ever-more complicated?

AS MUCH AS 90 PERCENT OF THE WORLD'S DATA HAS BEEN CREATED IN THE LAST TWO YEARS ALONE

Our advice will always be to focus on visibility. Only by establishing a complete view of exactly what data you have and where it lives can you implement the required policies to control how that data is used and ensure the right protections are in place.

That visibility will come from data discovery – a process in which all data repositories are scanned and evaluated to ensure all data is found, collected and consolidated. As you can imagine, this can be a comprehensive process. Microsoft has multiple different platforms that each store and use information in different ways – from SharePoint to OneDrive to Teams. Equally, with many companies now adhering to the 3-2-1 backup strategy (in which three copies of an organisation's data are kept on at least two different storage formats, with at least one kept off-site), it's common for firms to have numerous data repositories which need evaluating.

To do this manually would be a monumental and highly time-consuming effort, that simply would not be viable or even possible for most companies. Today, however, there are automated data discovery tools that can enable firms to locate PII and other data quickly and simply on a continuous basis, providing real-time insights across entire data landscapes.

That aspect of continuous monitoring is critical. If a car passes its MOT, only to pick up damage or a fault on the drive out, then it may not be road worthy for the next 12 months. In the case of data management, continuous monitoring ensures that things don't go awry, which could potentially lead to non-compliance. This is why visibility is so important. Having a knowledge base that serves as a single source of truth can help to flag issues or required remediations to administrators and data management professionals.

Here, automation again can pay dividends. Data discovery tools can be used to provide clear and accurate insights into an organisation's risk posture at any one time, for example, which can in turn be used to make informed governance decisions and demonstrate compliance to auditors and/or regulators.

On top of this, data classification tools can help companies to categorise their data, making it easier to ensure that the right protections are implemented. This is central to data management best practice.

Unstructured and unclassified data can often be the source of the biggest risks to organisations as they may be overlooked. By labelling data as confidential, PII or intellectual property, for example, firms can begin to build an index that makes it easier to implement and adjust data policies at scale.

With digital footprints and data landscapes continuing to become exponentially more complex, and the associated risks and threats growing by the day, organisations would be wise to implement these controls and work towards sustained compliance sooner rather than later.

GDPR WAS INTRODUCED TO GIVE INDIVIDUALS GREATER CONTROL OVER THEIR PERSONAL DATA

The DUAA is a welcome update to the existing GDPR legislation, alleviating the DSARs burdens that had been facing many firms. However, the core obligations that firms must adhere to haven't changed. Indeed, it's more important than ever for firms to have a clear and full understanding of what personal data they hold and how it is used.

Leveraging the right combination of automated data discovery and data classification tools is the easiest way to achieve this, giving firms the ability to more easily identify high-risk data, put the right safeguards in place and manage potential issues, changes or requests. However, not all such tools are made equal.

When it comes to selecting the right solutions, it's important to consider how they will fit into your existing structures and what your exact requirements are. It's worth considering whether data sovereignty is important to you, for example. If having a cloud-based solution raises concerns, then it's important to find the right tools that can be used on-prem.

Any data discovery or classification tools should also be easy to use from the get-go. If you can't clearly see how these tools function and ascertain the value that they can provide (be it automated reports or otherwise) in a short demo, then they are overly complex, and not the best fit.

In addition, it's also important to think about integration capabilities. Any tools should be compatible with your existing systems – be it Microsoft 365, Google Workspace, Alfresco, Atlassian, Confluence, your SIEM, critical APIs or otherwise. If it's not, then data discovery and classification won't be able to cover your entire data landscape, undermining compliance.

By asking the right questions, you will be well placed to find tools that complement your existing business processes and systems, supporting not only compliance but also helping to unlock competitive advantages. By definition, data discovery is the exploratory process of finding, collecting and analysing data, not only to manage risks, but also to uncover hidden patterns, trends and insights that can drive better business decisions, improve operations and make complex data understandable for all users.

While proper data hygiene is important, firms can also use the right tools to maximise the value of data. Consider PII – this is data that can be used to better understand your customers and provide more relevant and tailored services to them. According to a Deloitte survey, 80 percent of consumers surveyed prefer brands that offer personalised experiences and resultantly spend 50 percent% more with such companies. In this sense, data discovery and classification tools won't just help to alleviate compliance burdens. They can also act as a business differentiator, providing firms the platform from which they can operate smarter, innovate faster and differentiate from competitors ●

Michael Downs is VP at SecurEnvoy.

If having a cloud-based solution raises concerns, it's important to find the right tools that can be used on-site

Picture credit: AdobeStock