northdoor

◦ Store IT ◦ Protect IT ◦ Use IT ◦

Find and protect personal data

The vast number and variety of data repositories can make it difficult for organisations to track how and where personal data is stored. And how can you protect something when you don't know where it is? The Northdoor Data Discovery Service, based on GeoLang technology, automatically locates personally identifiable data and compiles the results in an executive report, making it quicker and easier to accurately locate personal data, reducing the risk of non-compliance with the data-protection legislation.

Where's my data? It's a deceptively simple question that many organisations struggle to answer.

Under both UK and EU law, individuals have the legal right to access, amend or delete personal information held by organisations. Individuals may issue a Subject Access Request (SAR) verbally or in writing at any time to find out what personal information an organisation holds, how it is being used, who it is shared with, and where the data comes from. Organisations have one month to respond. Failure to do so results in financial penalties for non-compliance.

According to the Commissioner's Office—the regulator overseeing data-proteciton enforcement in the UK—91 percent of organisations would fail to fulfil a SAR within the required timeline. This is because data is typically stored across a multitude of repositories, from endpoints, servers and external drives, to cloud applications and cloud storage. Put simply, many organisations do not know how or where their data is stored.

Northdoor has partnered with GeoLang, an award-winning cybersecurity solution provider, to solve this challenge.

Based on world-class GeoLang software, the Northdoor Data Discovery Service is designed to help organisations to locate, manage, protect and report on personal information. Built-in machine-learning algorithms enable Northdoor's team of experienced consultants to identify personal data across the corporate infrastructure both inside and outside the enterprise firewall.

The software searches for sensitive content, such as Personally Identifiable (PII), Payment Card Industry (PCI), HIPAA, and GDPR-related information, over a 30-day period. The findings are then compiled in an executive summary "HERO" report, which gives organisations a complete overview of their data—as well as their risk profile.

The HERO report provides detailed information on the types of data found, where it resides, whether it should be considered 'sensitive', and therefore whether the results constitute compliance with a framework standard such as the GDPR. This will help organisations to respond accurately and rapidly to SARs, and ensure effective remediation of potential risks and non-compliance.

Backed by dedicated, expert support from Northdoor, this comprehensive data discovery service will help organisations take control of their data—without breaking the bank.

Available as either a one-off scan or a continuous service, the Northdoor Data Discovery Service is the ideal foundation for data governance and information security policy implementation. As a result, your IT department can focus on enabling the business, while ensuring full compliance with the relevant data-protection legislation.

Once the SLAs are agreed, Northdoor deploys backup agents to all systems and sets up a single point of control in the cloud. Where enterprises are using backup solutions other than IBM Spectrum Protect, Northdoor handles the migration and provides a choice of backup target: either an existing storage system or an Accelerator built on IBM storage. In the latter case, Northdoor also provides this as a fully managed service, removing the storage management overhead.