

Major Telecommunications Organization

Full regulation compliance and data transparency with integrated suite of OpenText Data Privacy and Protection solutions.



Full Transparency in a Centralized Approach

In response to Europe's General Data Protection Regulation (GDPR), South Africa introduced PoPIA (Protection of Personal Information Act): South Africa's data protection law, aimed at protecting personal information processed by public and private bodies. As this organization has its roots in Europe and is committed to respecting its customers' and employees' data privacy globally, it aimed to not only meet the PoPIA regulation but to also introduce best practices from the GDPR rollout in Europe.

“The OpenText best-in-class portfolio offers superb integration, and the total is far greater than the sum of its parts. We feel we delivered a data management solution that can take our client far into the future. All data is searchable instantly in a cost-effective manner that always prioritizes the end-customer's privacy.”

Ken Wessels
Operations Director
Meniko

The organization sought advice from Micro Focus (now OpenText) and trusted partner Meniko who specializes in the security and management of data and records. Ken Wessels, Operations Director at Meniko, explains the scope of this undertaking: “Our client started this project with the aim of having an effective search capability across all structured and unstructured data. If the client can centrally manage customers' data preferences and usage permission, they could then respond swiftly to any customer data subject access requests (DSAR). This is an individual's right to request access to the personal information a company or organization holds on them. With many petabytes of customer and staff data to manage, locked in hundreds of applications and databases, this was no mean feat. We recommended OpenText™ data management and privacy solutions and OpenText Professional Services to collaborate in this effort.”

Cloud Migration Prompts More Structured Data Protection and Management

The project was triggered by a planned data migration to a cloud environment. The organization wanted to ensure that all redundant, obsolete, and trivial (ROT) data was clearly identified to avoid migrating more

At a Glance

Industry

Telecommunications

Location

Africa-wide

Challenge

Develop a central and unified data privacy and protection solution for global data privacy regulation compliance and faster DSAR response

Products and Services

Voltage Structured Data Manager (SDM)

IDOL

Content Manager

Success Highlights

- Drastically faster data searches in response to data subject access requests (DSAR)
- Facilitate PoPIA and GDPR compliance
- Optimization of unstructured data for cloud migration with significant data reduction through clean-up and deduplication
- Defensible deletion of expired data in a variety of databases
- Creation of Risk Rating reports for mitigating data breaches
- Encryption of sensitive data

data than was necessary. Prior to the cloud migration, the team aimed to clearly classify all business data. A key part of the data discovery project concerned unstructured data held in file shares, and the company's objective was to migrate this data to a shared storage environment.

OpenText and the Meniko team received a detailed business requirements specification from the client and converted this into a statement of work that the OpenText Professional Services team turned into a suggested framework, complete with full implementation guidelines. Workshops with the client started the analysis to identify data sources and network connectivity requirements. The workshops also served to introduce all departments to the data assessment and ensure a central level of understanding and support. The team secured executive sponsorship and worked directly with the customer program manager, the database administrators, application owners and other technical resources from the customer to create a comprehensive data inventory.

OpenText IDOL and OpenText Voltage Structured Data Manager (SDM) were deployed first in a test environment as part of a solution suite for a holistic, integrated, secure data protection and content management approach. Guided by an overall ruleset and priorities, the team started the planning to onboard over 700 applications to detect and classify personally identifiable information (PII) across unstructured and structured data so that this can be managed appropriately.

IDOL-Based Data Location Registry Supports Many Use Cases

Following the planning, design, build, and test phases, Meniko and the OpenText Professional Services team focused on scanning all structured data held in a variety of databases with SDM. Unstructured data, i.e., email, Office documents, and multimedia files, were scanned for PII through the IDOL engine so that any sensitive data could be identified. Working with each individual application owner, the data was extracted and deduplicated. It was then catalogued in an IDOL-based data location registry with clear pointers to applications and data sources where PII data may be found. From here, data could be searched, analyzed, and reported on through user-friendly dashboards.

"Before the OpenText implementation, we would have to query hundreds of systems, search for an individual's data, manually collate that data, and create a response to a DSAR. This could of course take hours, if not days." says Wessels. "Having this IDOL-driven register makes it easy to respond to a DSAR and manage data according to the individual's wishes."

Accurate Breach Impact Visibility through Application Risk Rating Reports

This increased visibility also supported the introduction of application risk rating reports. Having this risk assessment ensures accurate impact reporting in the case of a data breach.

Compliance to Cookie Consent

A data discovery project was launched to support a cookie consent audit. This involved the discovery of the client's many websites to give them a comprehensive list of all URLs in use. Leveraging IDOL connectors, this list was then compared to the list of websites to which the client had already applied cookie consent, to identify whether any URLs were missed.

Managing Expired Structured Data

OpenText Content Manager is used to implement effective data retention policies. By analyzing the huge data volumes, expired data within application databases could be detected automatically. As a result, the team could archive or delete a large amount of data, while carefully managing the remaining data to comply with data privacy regulations. Data optimization and minimization supports more streamlined data storage, shorter backup times, and saves overall on data management resources. A dedicated data privacy team from the client worked alongside Meniko and the OpenText Professional Services team. Through effective knowledge transfer, this team now has full in-house responsibility for ongoing regulation compliance. This includes producing data compliance reports so that application owners and the business can make informed decisions on how data is treated.

Wessels concludes: "The success of this project made our client an internal showcase for compliance. Through the great partnership with OpenText and its Professional Services team, we could deliver

“Our client started this project with the aim of having an effective search capability across all structured and unstructured data. If the client can centrally manage customers’ data preferences and usage permission, they could then respond swiftly to any customer data subject access requests (DSAR).”

Ken Wessels
Operations Director
Meniko

Connect with Us

www.opentext.com/products/security-cloud

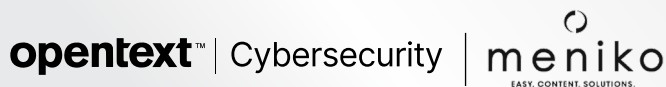


the data transparency our client needed. The OpenText best-in-class portfolio offers superb integration, and the total is far greater than the sum of its parts. We feel we delivered a data management solution that can take our client far into the future. All data is searchable instantly in a cost-

effective manner that always prioritizes the end-customer’s privacy. Our client was also pleasantly surprised to find that the OpenText data privacy solution could easily be extended into other areas of information governance, further increasing the investment value.”

Application	Business Process	Volume of Data	Nature of Data	Lawful Business	Scope of Access	Hasting	Supplier Data
Micro Focus RUM:ZA	Customer Experience Monitoring	Medium	Medium	Low	Low	Low	Low
Drupal Appl:ZA	Channel Content Management	Low	Medium	Medium	Medium	Medium	Low
Micro Focus BVD:Appl:ZA	Service Quality Management	Low	Medium	Medium	High	Medium	Low
Micro Focus OBR:Appl:ZA	Dashboard Reporting	Medium	Low	Medium	Medium	Low	Low
EPPIX:Appl:ZA	Customer Bill Charge Calculation	High	Medium	Low	Medium	High	Low
CDW Teradata:Appl:ZA	Integrated Data Warehouse	Low	Low	Medium	Low	Low	Low
Dispute & Reconciliation Management:Appl:ZA	Interaction Management	Low	Medium	Medium	Medium	Low	Low
Universal Content Management/WCC:Appl:ZA	Channel Content Management	Low	Low	Medium	Medium	Medium	Low
MSPI:Appl:ZA	Order Fulfillment Orchestration	Low	Medium	Low	Medium	Low	Medium
Voogel:Appl:ZA	Result Processing	High	Medium	Medium	Medium	Medium	Low
Oracle Siebel CRM:EBU:Appl:ZA	Operational CRM	-	Medium	Medium	Low	Low	Medium
Genesys:Appl:ZA	IP Multimedia Contact Centre	Low	Medium	Medium	Medium	Medium	Low
Nimble:Appl:ZA	Collaboration Tools	Low	Medium	Low	High	High	Low
Leavers Management Workflow:Appl:ZA	Collaboration Tools	Low	Low	Medium	Medium	High	Medium

Figure 1. Application Risk Report required for mitigation of a data breach



OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.