OpenText Core Data Discovery & Risk Insights (Voltage) powers data privacy

Australian organisations must now balance innovation with stricter Privacy Act (1988) rules, updated in 2024–2025, using advanced privacy-enhancing technologies

Benefits

Privacy compliance

- Identify and manage sensitive and personally identifiable information (PII) across your data estate

Advanced privacy-enhancing technology

- Act on data during discovery to accelerate decision-making and build data trust

Beyond compliance

- OpenText supports data minimisation, secure analytics, lifecycle governance, and sustainability goals

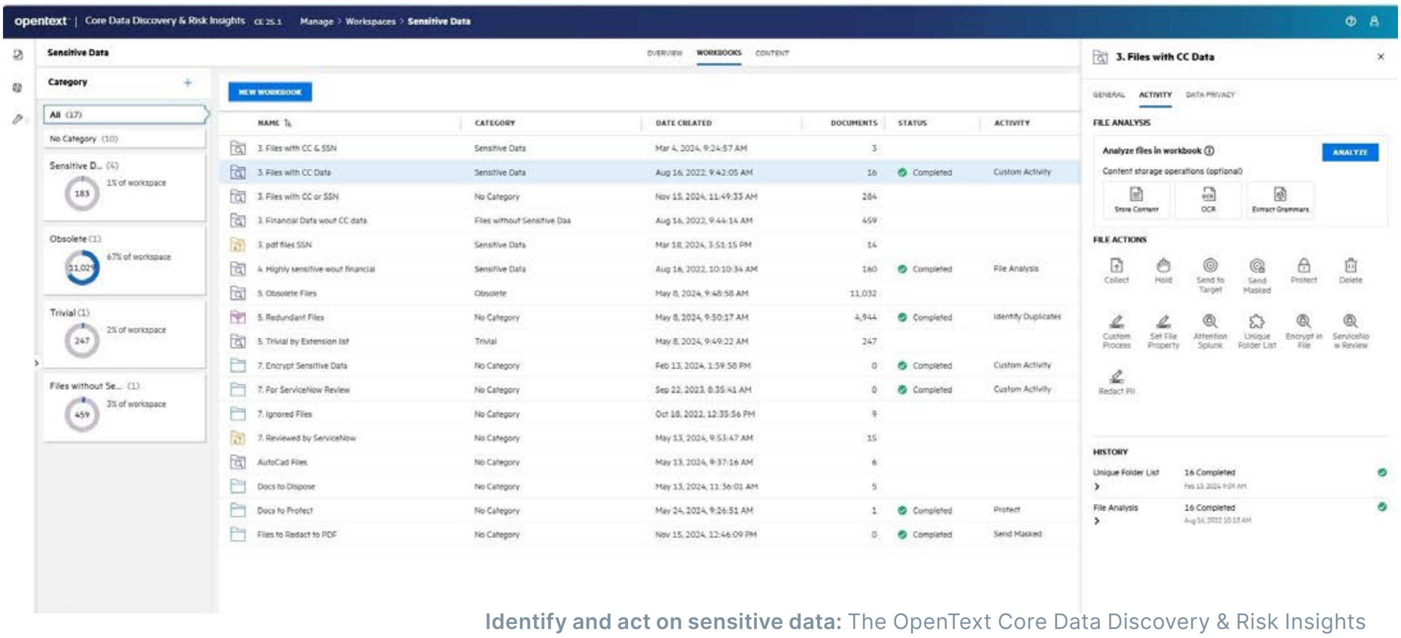
Australia's updated Privacy Act demands more than basic compliance. As rules tighten and public expectations rise, organisations must rethink how they manage sensitive data. OpenText™ Core Data Discovery & Risk Insights (Voltage) helps address these challenges with advanced privacy-enhancing technologies that turn risk into resilience.

The most secure information management platform

By combining the strengths of OpenText Content Management and OpenText Cybersecurity, organisations gain access to the most secure information management platform in the market. This integrated approach ensures that sensitive data is not only well-governed and discoverable but also protected against evolving cyberthreats—across its entire lifecycle.

Together, these capabilities deliver:

- Unified governance and security across content and data.
- Persistent protection from creation to deletion.
- Resilience against breaches, insider threats, and regulatory non-compliance.
- Confidence in data integrity, availability, and ethical use.



NAME	CATEGORY	DATE CREATED	DOCUMENTS	STATUS	ACTIVITY
3. Files with CC & SSN	Sensitive Data	Mar 4, 2024, 9:24:57 AM	3		
3. Files with CC Data	Sensitive Data	Aug 16, 2022, 9:42:05 AM	16	Completed	Custom Activity
3. Files with CC or SSN	No Category	Nov 15, 2024, 11:49:33 AM	284		
3. Financial Data wout CC data	Files without Sensitive Daa	Aug 16, 2022, 9:44:14 AM	459		
3. pdf files SSN	Sensitive Data	Mar 18, 2024, 3:51:15 PM	14		
4. Highly sensitive wout financial	Sensitive Data	Aug 16, 2022, 10:10:34 AM	160	Completed	File Analysis
5. Obsolete Files	Obsolete	May 8, 2024, 9:48:58 AM	11,032		
5. Redundant Files	No Category	May 8, 2024, 9:50:17 AM	4,944	Completed	Identify Duplicates
5. Trivial by Extension list	Trivial	May 8, 2024, 9:49:22 AM	247		
7. Encrypt Sensitive Data	No Category	Feb 13, 2024, 1:59:58 PM	0	Completed	Custom Activity
7. For ServiceNow Review	No Category	Sep 22, 2023, 8:35:41 AM	0	Completed	Custom Activity
7. Ignored Files	No Category	Oct 18, 2022, 12:35:56 PM	9		
7. Reviewed by ServiceNow	No Category	May 13, 2024, 9:53:47 AM	15		
AutoCad Files	No Category	May 13, 2024, 9:37:16 AM	6		
Docs to Dispose	No Category	May 13, 2024, 11:36:01 AM	5		
Docs to Protect	No Category	May 24, 2024, 9:26:51 AM	1	Completed	Protect
Files to Redact to PDF	No Category	Nov 15, 2024, 12:46:09 PM	0	Completed	Send Masked

Unique Folder List — 16 Completed — Feb 13, 2024 9:09 AM

File Analysis — 16 Completed — Aug 16, 2022 10:13 AM

Identify and act on sensitive data: The OpenText Core Data Discovery & Risk Insights dashboard shows categorised workbooks, file analysis status, and data protection actions.

Aligning with Australia's privacy principles

The Privacy Act 1988, as amended, introduces new rights and responsibilities, including:

- The right to access, correct, and delete personal information.
- Stronger protections for children's data and automated decision-making transparency.
- Obligations to minimise data collection, limit retention, and safeguard cross-border data transfers.
- A new statutory tort for serious invasions of privacy and enhanced OAIC enforcement powers.

OpenText Core Data Discovery & Risk Insights helps organisations operationalise these principles through:

Cross-border data transfers and sovereignty

Australia is introducing a "white list" mechanism for international data transfers, requiring stronger due diligence on overseas data handling and clear documentation of data flows and processing locations. OpenText Core Data Discovery & Risk Insights supports compliance with data privacy, residency, and cross-border data transfer requirements by enabling data sovereignty enforcement through sovereign cloud infrastructure deployed in region. It enhances regulatory alignment through regulation-specific PII detection, tagging, and system-of-origin tracking, ensuring that personal data is identified, governed, and appropriately restricted or transferred based on jurisdictional rules. Mitigating measures, such as privacy-preserving technologies (e.g., encryption, anonymisation), are applied to reduce transfer risks, while built-in compliance reporting provides transparency and auditability across data flows.

"OpenText Core Data Discovery & Risk Insights has taken us on an incredible journey with surprises at every turn. We have found real treasures among our millions of files, as well as ways to drastically reduce our storage costs and safeguard the sensitive data that is our museum's legacy."

Kerry Cody
Head of Digital and Information Services, Queensland Museum

Privacy-enhancing and privacy-preserving technologies

- **PII detection and classification:** Discover and classify personal and sensitive data across structured and unstructured sources.
- **Anonymisation and de-identification:** Reduce identifiability of individuals while retaining data utility for analytics.
- **Encryption and access controls:** Protect data at rest, in motion, and in use, ensuring only authorised access.
- **Data minimisation and retention governance:** Collect only what's necessary, retain only as long as needed, and dispose of data defensibly.
- **Clean document renditions for GenAI pipelines:** Automatically generate redacted, structured, and context-aware versions of documents that are optimised for ingestion into generative AI workflows—ensuring privacy, compliance, and data quality.

Building privacy-first resilience for critical infrastructure

As Australia strengthens its national cybersecurity posture, data privacy, and infrastructure resilience are converging as dual priorities under regulatory and operational mandates. The Security of Critical Infrastructure (SOCI) Act and ACSC's Essential Eight framework are now integral to how organisations—particularly those in sectors such as healthcare, finance, energy, and telecommunications—manage and secure their data.

OpenText Core Data Discovery & Risk Insights empowers critical infrastructure providers to meet these standards by integrating data privacy-by-design into their security strategy and helps shift from a reactive to proactive maturity. Proactively discovering, classifying, and governing sensitive information—particularly personal and operational data—enables organisations to embed privacy principles while addressing Essential Eight priorities, such as restricting administrative privileges, implementing multi-factor authentication, and managing application patches and configurations.

OpenText's strength is helping customers understand and manage data. OpenText is the ideal partner for supporting critical infrastructure mandates, augmenting risk management programs and bridging operational technology and IT environments.

With a unified platform, OpenText supports Essential Eight strategies through persistent protection of sensitive data, lifecycle management for compliance and recovery, and automated anomaly detection to bolster threat response. These capabilities not only meet privacy obligations under the Privacy Act and ISO 27701, but also establish operational resilience demanded by Australia's evolving security landscape.

Key use cases mapped to Australian privacy obligations

Right to delete
Business purpose
Data minimisation
Data protection
Data portability

The Right to Delete—Australian Privacy Principles (APPs) 11.2

The APP 11.2. requires entities to take reasonable steps to destroy or deidentify personal information when it is no longer needed for any purpose for which it may be used or disclosed under the APPs.

OpenText Core Data Discovery & Risk Insights enables the defensible disposition of personal information in accordance with policy, right to be forgotten, or other data deletion requests.

Business Purpose—Australian Privacy Principles 3 and 6

The APPs 3 and 6 outline that personal information should only be collected, used, or disclosed when it is directly necessary for the entity's functions or activities—essentially, its legitimate business purpose. This ensures the data is only handled in ways that align with the stated purposes and limits unnecessary or excessive data use.

Our data security solutions can understand where duplicate and low-value data resides and assign retention policies and tagging to ensure ethical handling and processing of personal information.

Data Minimisation—Australian Privacy Principles 3 and 11

The concept of data minimisation is mentioned throughout the APPs, particularly in APP 3 and 11. APP 3 states that entities must only collect personal information that is reasonably necessary for their functions or activities. In parallel, APP 11 requires entities to take reasonable steps to protect personal information from misuse and to destroy or de-identify it when it is no longer needed. As a result, personal information deemed "necessary" must have a specific business use and retention period.

Our capabilities support data minimisation efforts that reduce the cost and complexity associated with application and data sprawl. These use cases include application retirement and modernisation, cloud migrations and data archiving. In addition, OpenText Core Data Discovery & Risk Insights ensures that only the appropriate data is retained to support audit, legal and regulatory obligations.

Data Security and Protection—Australian Privacy Principle 11

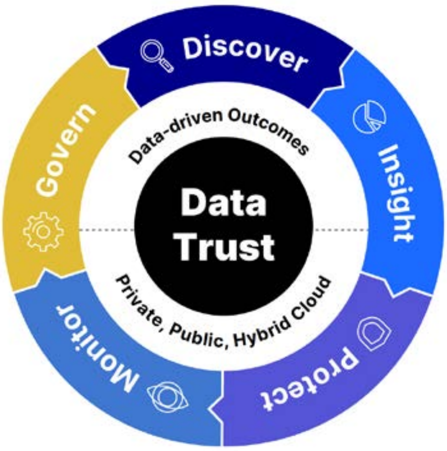
The APP 11 states that a business that collects personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorised or illegal access, destruction, use, modification, or disclosure.

From a privacy compliance standpoint, our solution can enable businesses to monitor data access and implement de-identification and encryption as technical safeguards to protect personal information and corporate reputation in case of a breach.

Data Portability—Australian Privacy Principle 12

The APP 12 states businesses that receive a consumer request to access their personal information shall promptly disclose and deliver it.

Our platform search capabilities can quickly find associated personal information and package responsive data as required to support data portability requests.



Resources

- OpenText Core Data Discovery & Risk Insights

The OpenText Data Discovery & Risk Insights governance framework

- **Govern:** Apply lifecycle policies, automate defensible deletion, and respond to DSARs and Notifiable Breach Schemes.
- **Monitor:** Track data access, detect anomalies, and enforce rights.
- **Discover:** Build a data inventory with context-aware discovery of PII and sensitive data.
- **Insight:** Visualise risk, assign business purpose, and prioritise remediation.
- **Protect:** Enforce persistent protection, privacy by design, and data sovereignty.

A platform driving business outcomes beyond compliance

Secure cloud analytics

Enable privacy-preserving analytics across platforms like Snowflake®, Google BigQuery™, and Microsoft® Azure Synapse Analytics using protected data.

Financial risk visibility

Quantify the economic impact of data risk and inform cyber insurance strategies.

Sustainability and green IT

Reduce storage and energy consumption by eliminating unnecessary data and modernising legacy systems.

Standards alignment

OpenText Core Data Discovery & Risk Insights supports compliance with national and state-based privacy regulations along with ISO 27701, the privacy extension of ISO 27001, through capabilities such as:

- Privacy impact assessments
- Ethical records of processing
- Data minimisation and deletion
- Data portability and protection

OpenText Core Data Discovery & Risk Insights provides a comprehensive, privacy-enhancing solution aligned with Australia's modernised privacy regime. When combined with OpenText Content Management and OpenText Cybersecurity, it delivers the most secure and trusted information management platform available—empowering organisations to reduce risk, build trust, and unlock value from data—ethically and sustainably.