NUIX NEO DATA PRIVACY FOR DATA BREACH READINESS

Government organizations are a prime target for cyber-attacks given they manage highly sensitive information, from classified intelligence to personal, health, and financial details of citizens. Nuix Neo Data Privacy helps you locate, classify and protect information, to maintain public trust in a high-risk landscape.

SAFEGUARDING PUBLIC TRUST

Many government organizations will be impacted by a data breach due to the sensitive nature of the data they hold — from tax records and identity information to defense and public health. **In 2023, ransomware attacks on public sector organizations increased by 40 per cent.**[1]

Sensitive data is often siloed across departments and agencies, making it hard to map exposure or identify vulnerabilities. Challenges in inter-agency communication and limited oversight of third-party risks further complicate breach-readiness.

With cyberattacks on the rise, protecting sensitive data is essential for service continuity and public trust. **In 2024, data breaches averaged US$4.88 million, up 10% from the previous year**, bringing not just financial loss, but also operational disruption and reputational damage.

Government organizations need full visibility into their data and a strong, proactive approach to breach readiness.

OUR SOLUTION

Nuix Neo Data Privacy gives government organizations visibility and control over their data landscape. Stay compliant with stringent regulations like, GDPR, FISMA (US), LGPD (Brazil), PDPA (Singapore), the Australian Privacy Act 1988, and PIPEDA (Canada), avoid costly fines, and reduce the fallout from potential data breaches.

With Nuix Neo Data Privacy, you can:

IDENTIFY
Pinpoint PII and sensitive data across complex, silioed internal systems, cloud storage and third-party providers, focusing on areas with the highest risk.

ANALYZE
Leverage automated reports to enhance governance, compliance, and risk management practices.

MINIMIZE
Remove outdated data, and separate sensitive information — including citizen data, plans, and confidential details, ensuring only critical information is retained for audits or legal purposes.

ACT
Implement proactive measures to secure sensitive data, ensure regulatory compliance and reduce the threat of unauthorized access.

THE OUTCOME
Maintain compliance and protect public trust with Nuix Neo Data Privacy.

Harness cutting-edge automation, Cognitive AI, and precision data discovery and classification to safeguard sensitive citizen information, ensure regulatory compliance, and **uphold citizen confidence**.

---

1   https://www.itsecurityguru.org/2024/01/23/public-sector-cyberattacks-rise-by-40-in-2023/

KEY FEATURES OF NUIX

Responsible AI: Nuix Neo Data Privacy uses advanced AI to analyze over 1,000 file types quickly and accurately. It automates reading and prioritizing unstructured data for faster insights.

Out-of-the-Box and Custom AI Models: Nuix Neo Data Privacy includes 500 prebuilt AI models to accelerate your data breach readiness processes – plus no-code tools to easily create models tailored to your specific needs.

Data Discovery & Classification: Easily search and classify government data across systems to identify, label, and protect sensitive information.

Automated Risk Insights: Generate automated reports that reveal areas of high sensitivity so you can proactively eliminate vulnerabilities, meet compliance requirements, and protect critical assets.

Automatically Identify PII

Case Summary Report

Summary	Value	
Generated By	cstiller01	
Generated On	2023-07-24 09:35	
Case Name	PodestaMBOX	
Production Set	Production00001	

Entity Count

Entity	Item Count	Audited Size
bank-account-number	0	0 bytes
credit-card-number	14	550.254 kB
credit-card-information	0	0 bytes
cvv	4	104.403 kB
date-of-birth	70	25.631 MB
drivers-license	0	0 bytes
mothers-maiden-name	15	5.443 MB
password	2870	390.989 MB
pin-number	3	7.687 kB
ssn	10	7.027 MB
swift-code-bic	10	1.778 MB
tax-id-number	114	6.395 MB
username	96	11.058 MB

WHEN DATA IS LOST

In 2023, a **UK public-sector organization** responsible for managing sensitive citizen data experienced a breach that **exposed personal details of over 40 million individuals**. The incident went undetected for several months, which sparked questions about the integrity of democratic infrastructure and the adequacy of national cyber readiness.

In Australia, a **large state-based government agenc**y[2] was compromised through a phishing attack on employee email accounts, **exposing 500,000+ documents containing identity and contact data**. The incident led to a class action and intensified scrutiny on public sector data governance.

In the US, **a file transfer software breach**[3] impacted dozens of federal and state agencies, including the Department of Energy and public education systems. **Sensitive files were published online**, fueling concerns about third-party software vulnerabilities.

---

2   Source: Service NSW data breach
3   Source: MOVEit software breach

WHO NEEDS THIS SOLUTION?

Assess the value of Nuix Neo Data Privacy for your organization with these key questions:

> Do you know where sensitive, confidential and personal information is stored?

> Are you confident that no national, classified or personal information is stored in unsecure locations within your government systems?

> Are you equipped to assess data across multiple, typically siloed, departments and mitigate risks quickly in the event of a breach?

> Do you have a clear understanding of your data ecosystem, and can remain compliant with all privacy laws, including GDPR?

> Can your department respond quickly and effectively to a data breach?

Speak to us today to find out more **nuix.com/contact-us**