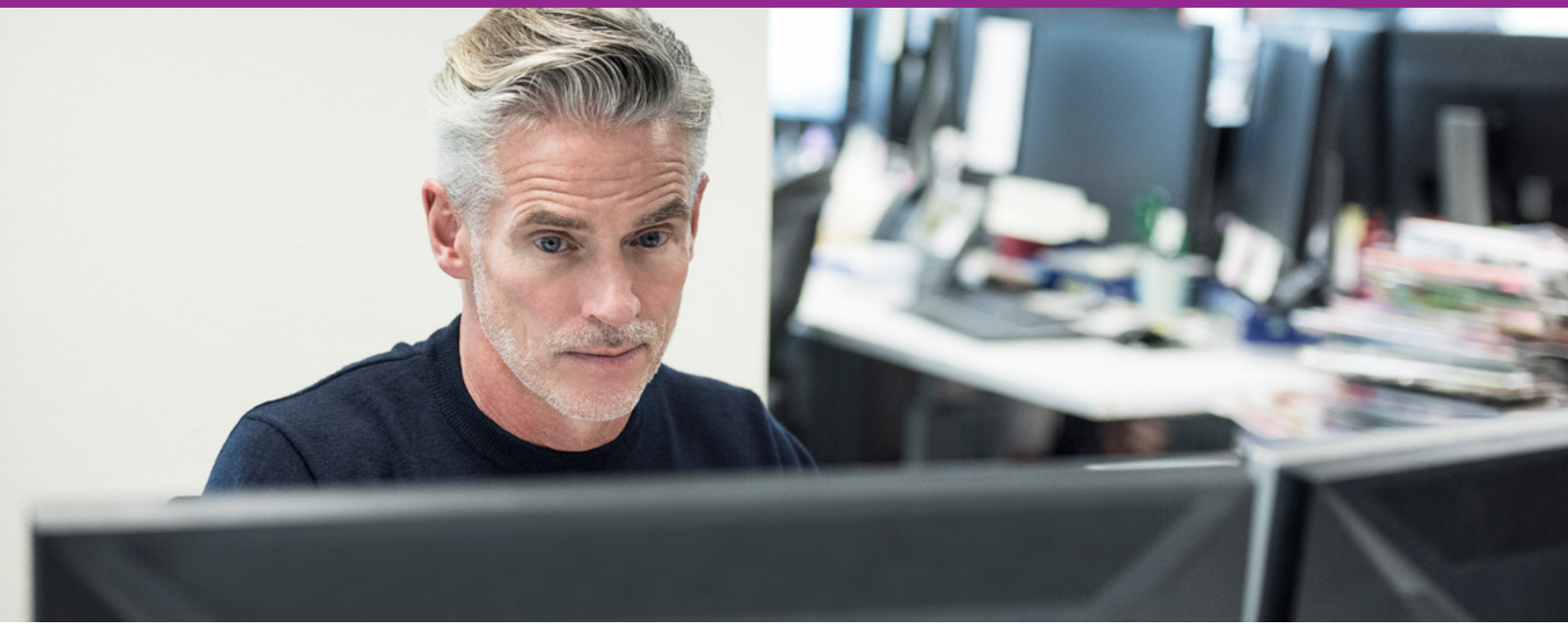
nuix

BUILDING A COMPLETE REGULATORY COMPLIANCE PROGRAM



THE COMPLIANCE CHALLENGE - IDENTIFY, MANAGE, AND MONITOR PERSONALLY IDENTIFIABLE INFORMATION.

Data privacy and other regulations significantly restrict organizations' ability to process personally identifiable information (PII).

Organizations that retain personal information will need to understand and comply with a potentially broad range of data protection regulations. Failing to comply can lead to urgent business issues and economic hardship.

Companies are trying to understand how to prepare. Some companies are hiring Data Privacy Officers, some are inventorying their data, and some are updating their information governance policies around PII.

As legal precedents continue to be set and evolve, companies need to respond to the latest information and have a full solution in place.

Simply put, there are three sides to the foundation of regulatory compliance.

PEOPLE. Companies need to hire and assign the right people, including a Data Privacy Officer or similar role, to focus on and be accountable for regulatory compliance.

PROCESS. Businesses need to create and update information governance policies and data management processes to administer requests and regulatory needs.

TECHNOLOGY. Corporations must identify, manage, and monitor their data to build the foundation of information needed to comply with the regulations.

SEVEN QUESTIONS TO START BUILDING YOUR COMPLIANCE FOUNDATION

If technology alone is not the answer, what is? The answer lies in intelligently applying technology, smart processes, and support to help meet your regulatory requirements. Companies and their consultants updating policies and procedures can improve their compliance posture by answering these seven questions.

WHAT KINDS OF PERSONAL DATA DO YOU HAVE?

Data privacy and other regulations include broad definitions of personal data. Some data types will match simple patterns; others are more complex and require validation. Some will be very subjective and require full-text analytics and classification. A Nuix analysis of a sample data set will show you what you have and how best to find or remediate it.

WHERE IS IT LOCATED?

A data map is a valuable part of any information governance project. A content inventory shows you where to look for, govern, and protect personal data. It also highlights content repositories where there is little or no risk. Nuix's parallel processing can plow through massive volumes of data and help map high-, medium-, and low-risk data assets.

HOW DO YOU ARCHITECT A SYSTEM TO BEST MANAGE IT?

Once you know what and where personal data is and architecting the ideal solution is a matter of selecting the best deployment options to minimize risk and maximize finding data. Considerations include deployed agents, database back end, web or client interface, indexing speed, analytics capabilities, review efficiency, and defensible actions.

WHAT PEOPLE AND PROCESSES DO YOU NEED IN PLACE?

Responsibility for compliance often falls to one person within the organization, but they won't be working alone. You need to get the right information to the right people so they can understand content, review risk, and find methods and sources. This requires ease of use and ease of deployment. Nuix can help identify expertise and target activities.

HOW DO YOU APPLY INFORMATION GOVERNANCE REMEDIATION?

The evidence you need is already in the existing data; therefore, you need to build privacy by design into new and current policies and procedures. Nuix can identify unprotected personal data, where it comes from, and why it's there. Most importantly, you can act on that data to remove the risk or change the process by using Nuix to carry out the required workflows with ease and precision.

HOW DO YOU ACTIVELY PROTECT THE DATA?

Companies need vigilance to ensure regulatory compliance. Using Nuix enables an 'always on' approach, enabling you to detect multiple attack vectors, drive lab testing, and support various potential incident response techniques to stop cybersecurity threats and breaches in real time.

HOW DO WE PROVIDE PROOF WE ARE HANDLING PII APPROPRIATELY?

You need to show regulators that you are in control of, and protecting, private information. Nuix software enables you to accurately report breaches and the handling of PII to the company board and regulatory authorities while swiftly executing subject access requests, right to erasure, and other information requests.

REGULATORY PROCESS FLOW

There are seven questions to ask your customers about how they handle and protect data. Once you know where they stand, follow this simple cycle to ensure continued compliance with applicable regulations, all powered by Nuix software.

THE BUSINESS CASE FOR ALWAYS ON VISIBILITY

Making information governance a core practice brings many advantages, including business agility and brand security. It also makes good business sense. With strong information governance in place, you can reduce the costs of subject access requests, respond rapidly to ad hoc regulatory audits, and avoid unnecessary audits and fines.

Seeing no evil is no longer a valid excuse for poor data management. The ability to see more and act faster has never been so valuable.

THE BUSINESS CASE FOR NUIX

There is one proven, forensic-grade information governance solution out there: Nuix.

Nuix's always on approach to data management is used by hundreds of organizations globally, including large corporations, law enforcement agencies, government regulators, service providers, and legal organizations.

Nuix delivers state of the art data protection, quick and seamless response to information requests, and intelligent processing as the best information processing engine in the world.

Ensure complete visibility while moving to action with our Always On approach.

WHAT IS PERSONAL DATA ANYWAY?

Personally identifiable information can come in many forms. For example, the European Union General Data Protection Regulation defines personal data as “Any information related to an identified or identifiable natural person.” This definition may include more than you think.

- **DIRECT IDENTIFIERS**
  Name, identity number, account number, physical address
- **ONLINE IDENTIFIERS**
  Social media handle, email address, profile picture, avatar, screen background
- **INDIRECT IDENTIFIERS**
  Religion, political persuasion, sexual orientation, hobbies, genetic profile
- **HIGHER PROTECTION**
  Personal data that reveals racial or ethnic origin; political, religious, or philosophical beliefs; biometrics; and genetic data about health, sex life, or sexual orientation can all be considered PII. Many times, these identifiers can’t be determined ahead of time and don’t follow a specific format, as with the other examples listed here. Nuix provides a variety of wasy to search, group, compare, and categorize more ambiguous or subjective content.

To find out more about Nuix for data privacy, visit

nuix.com/problems-we-solve

nuix

Nuix understands the DNA of data at enormous scale. Our software pinpoints the critical information organizations need to anticipate, detect, and act on compliance, risk, and security threats. **To learn more visit www.nuix.com**.

APAC

Australia: +61 2 8320 9444

EMEA

UK: +44 203 934 1600

NORTH AMERICA

USA: +1 877 470 6849