FORTRA®

DATASHEET (FORTRA)

Fortra for NATO STANAG Conformance

Fortra's Data Classification Suite provides the classification labelling, metadata binding, and policy enforcement capabilities that NATO STANAG 4774 and 4778 require, giving allied organizations a practical, scalable path to data-centric security conformance.

The Challenge of NATO STANAG Conformance

NATO's 32 member nations and over 40 partner countries depend on shared classification standards to share intelligence, coordinate operations, and communicate securely. STANAGs 4774 and 4778 define the technical foundation of that shared standard — specifying how sensitive information must be labeled with machine-readable confidentiality metadata, and how those labels must be bound to the data they protect. The framework is clear; execution is often where organizations struggle.

Because member and partner nations each maintain their own national classification schemas alongside NATO's, the metadata applied to shared information must reflect an ever-shifting reality: which countries belong to which groups at the time a document is created, what classification levels and releasability markings apply, and how those labels should be interpreted by systems operating under different national policies. Without purpose-built tools, users apply markings inconsistently, and metadata is misunderstood as data moves between systems.

Common obstacles to STANAG 4774 and 4778 conformance include:

Inconsistent manual classification. When classification is left to individual users without guided tooling, markings are applied inconsistently across documents, emails, and files, creating the gaps in confidentiality labelling that both STANAGs are designed to close.

Metadata loss across systems. Labels that are not persistently embedded in the data itself can be stripped or lost as files move between systems, coalition networks, and cloud environments, undermining the data-centric security model that STANAG 4774 enables.

Schema complexity across member nations. NATO group membership changes over time, and metadata must capture the identity of member nations at the time of document creation. Managing this complexity manually is error-prone and unsustainable at scale.

SOLUTION SUMMARY

Fortra's STANAG conformance solutions make it easy to:

- Apply STANAG-relevant classification labels
- Embed persistent confidentiality metadata in files
- Classify consistently across coalition environments
- Enforce DLP policies based on classification metadata
- Support unlimited NATO and national label schemas
- Apply portion marking to multi-classification documents
- Integrate with existing security infrastructure

Our Solution

Fortra Data Classification provides a common classification and policy solution designed specifically for the complexity of NATO's information sharing environment. With support for STANAG 4774-compliant confidentiality label syntax and STANAG 4778 label binding, DCS gives organizations the technical capability to conform to both standards — consistently, across every user and every file type.

Classification, Labeling, and Metadata

Our solution enables users to apply PSPF and NATO-aligned classification markings across Microsoft 365, Outlook, and Windows, with persistent metadata embedded in every document and email. Classification labels are stored as structured metadata consistent with STANAG 4774's confidentiality label syntax — including policy identifier, classification level, releasability markings, and creation timestamp — ensuring that labels carry the full context downstream systems need to enforce access decisions.

The classification experience is designed to reduce human error. Guided classification prompts walk users through the labelling process with suggestions based on content detection, while policy tips prevent over- or under-classification. Administrators can configure unlimited classification labels to reflect NATO schemas, national classification systems, and coalition-specific requirements — including portion marking at the paragraph, table, or image level for complex multi-classification documents.

Label Binding, Integrity, and Downstream Enforcement

Conformance with STANAG 4778 requires that a label is bound to content consistently for all implementations, thus ensuring interoperability. Fortra DCS supports label binding using the STANAG 4778 profiles.

Beyond the label itself, Fortra Data Classification integrates with downstream security tools to put classification metadata to work. Fortra DLP, for example, can read DCS metadata to enforce data handling and sharing policies. ACP 240 implementations, ABAC and access control systems can use label attributes to make automated access decisions. And Fortra DSPM extends classification-aware visibility to cloud and hybrid environments, maintaining an inventory of labelled data holdings across the organization. The result is a connected, metadata-driven security posture — with STANAG-conformant labels as the foundation.

STANAG	PRIMARY REQUIREMENT	FORTRA DATA CLASSIFICATION CAPABILITIES	MORE FORTRA CAPABILITIES
STANAG 4774	Provide common XML-based syntax for confidentiality metadata labels that identify the classification, releasability, and handling requirements of NATO information objects, enabling automated, policy-driven access decisions based on the data itself.	• STANAG 4774-compliant confidentiality label syntax • Persistent metadata embedding across all supported file types • Unlimited classification labels for NATO, national, and coalition schemas • Portion marking • Visual markings (headers, footers, watermarks) • Guided classification with policy tips and suggested labels	**Fortra DSPM** Automatic classification label application upon sensitive data discovery across cloud and hybrid environments **Fortra DLP** Classification metadata-driven policy enforcement across endpoints, networks, and cloud environments
STANAG 4778	Define a standardized mechanism for binding metadata to information objects throughout their lifecycle, enabling trust between sharing partners across systems and coalition networks.	Persistent metadata-based binding maintained as data moves across partner systems, networks, and cloud environments	**Fortra DLP** Enforcement of data handling policies based on classification metadata, preventing unauthorized transmission of labelled information

FORTRA

Fortra.com