FORTRA

DATASHEET

# Navigating Saudi Data Regulations with Fortra

## Data Security Solutions for PDPL and NDMO Compliance

As the Kingdom of Saudi Arabia accelerates its digital transformation under Vision 2030, data has become a national asset requiring strict governance and protection. For organizations operating within the Kingdom, compliance is no longer achieved through passive data storage or perimeter security alone. Instead, it requires a shift toward active data management and continuous personal data protection across the entire data lifecycle.

Regulatory frameworks such as the Personal Data Protection Law (PDPL) and the National Data Management Office (NDMO) standards now impose clear obligations on how organizations classify, protect, transfer, and monitor data. Together, these frameworks mandate:

- Data identification and classification
- Risk and impact based protection controls
- Secure data processing, storage, and transfer
- Data minimization and retention enforcement
- Incident detection and notification
- Cross-border data transfer restrictions and controls

Fortra addresses these requirements through an integrated approach that combines Fortra Data Classification and Fortra Data Loss Prevention (DLP), delivering technical controls that align directly with PDPL articles and NDMO domains.


**EXECUTIVE SUMMARY**

The integrated deployment of Fortra Data Classification and Fortra DLP provides a unified compliance framework supporting PDPL and NDMO regulatory requirements via:

- Automated discovery
- Impact-based classification
- Persistent metadata enforcement
- Encryption and egress protection
- Lifecycle governance
- Real-time breach detection
- Audit-ready reporting

This layered approach establishes a defensible, regulator-aligned, and technically enforceable compliance posture for organizations operating within the Kingdom of Saudi Arabia.

## Data Discovery, Identification, and Inventory

### PDPL Articles 10 and 11 | NDMO Domain 9.13

Fortra Data Classification detects Saudi-specific data identifiers such as national ID, IQAMA, and passport information. It compares user-identified classifications versus suggested classifications and reports on file location and encryption status to support data-at-rest requirements.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Art. 10 and 11 | DC.3.1 | Identify and inventory Personal Data and datasets | Scanning file repositories | Scan Overview Dashboard |
| Art. 10 and 11 | DC.3.1 | Detect unclassified sensitive data | Privacy Catalogue (Saudi ID, IQAMA, Passport detection) | Detected Content Reports |
| Art. 10 and 11 | DC.3.1 | Maintain a record of data locations | Data-at-rest inventory | Inventory Report |

## Classification and Impact Assessment

### PDPL Article 10 | NDMO Domain 9.13

Fortra Data Classification offers guided classification assistance to prevent misclassification. It enables NDMO-compliant classification schemes such as Public, Restricted, Secret, and Top Secret. Classifications are written as persistent metadata, ensuring they travel with the data.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Art. 10 | DC.3.2 | Assign classification based on impact | Configurable schema (Top Secret, Secret, Confidential, Public) | Classification Policy Configuration |
| Art. 10 | DC.3.2 | Prevent misclassification | Policy tips and auto-upgrade based on detection | Classification Enforcement Logs |
| Art. 10 | DC.3.2 | Publish classification as metadata | Metadata injection (Office properties, email headers) | File Properties Metadata |
| Art. 10 | DC.3.2 | Ensure classification persistence | Alternate data stream tagging | Kernel-Level Tag Verification |

## Disclosure Prevention and Access Control

### PDPL Articles 15 and 16 | NDMO Domain 9.13

Fortra DLP keeps data out of the wrong hands. Block uploads to unauthorized cloud services and restrict external file transfers, restrict screenshots and copy/pasting of sensitive data, and prevent unauthorized applications and malware from accessing your data.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Art. 15 and 16 | DC.2.1 | Prevent unauthorized disclosure | Network transfer upload (NTU) blocking | Policy Violation Logs |
| Art. 15 and 16 | DC.2.1 | Restrict data access to authorized applications | Trusted process and application control | Access Enforcement Logs |
| Art. 15 and 16 | DC.2.1 | Prevent data leakage via clipboard/screenshots | Clipboard control and screen capture monitoring | Incident Investigation Records |

## Encryption and Secure Handling

### PDPL Article 19 | NDMO Domain 15

Protect data in case of device loss or attempts to copy classified data to a USB with Fortra DLP's automated AES-256 encryption. Its location-aware enforcement also applies stricter policies when users are on public networks or working remotely.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Art. 19 | DC.2.1 | Protect data during transfer | Removable media encryption AES-256 | Encryption Status Report |
| Art. 19 | DC.2.1 | Risk-based protection measures | Location-aware policy enforcement | Policy Configuration Evidence |
| Art. 19 | DC.2.1 | Prevent exfiltration via unauthorized channels | Egress filtering and domain control | NTU Blocking Reports |

## Data Retention and Destruction

### PDPL Article 18 | NDMO Governance Requirements

Monitor file deletion activity with Fortra DLP, which provides audit evidence of authorized data disposal. It also automatically moves improperly stored data, documenting secure handling and lifecycle control.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Art. 18 | Governance Controls | Destroy data when no longer required | File delete monitoring | Deletion Audit Logs |
| Art. 18 | Governance Controls | Prevent improper storage | Quarantine (data vaulting) | Quarantine Action Reports |

## Personal Data Protection and Assessment

### PDPL Core Principle | NDMO Domain 9.14

Fortra DLP detects Saudi-specific PII patterns and identifies PII datasets automatically. When sensitive data patterns are detected, it can automatically tag the file, apply protection policies, or block unauthorized actions — ensuring PDPL protection is enforced by design, not by user behavior alone.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Core PDPL Principle | PDP.1.1 | Identify types of personal data collected | Privacy catalogue | PII Detection Reports |
| Core PDPL Principle | PDP.1.1 | Identify storage locations | Repository mapping | Storage Location Dashboard |
| Core PDPL Principle | PDP.1.1 | Evaluate processing risk | Endpoint inspection | Risk Activity Logs |

## Data Breach Detection and Notification

### PDPL Article 20 | NDMO Domain 9.14

Get real-time, high-fidelity alerts on mass file exports and other policy violations. These Fortra DLP alerts include timestamps, user identities, and specific rule violation notes. Enterprise forensics enable detailed reporting and timely regulatory notification and impact analysis.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Art. 20 | PDP.3.1 | Detect personal data compromise | Real-time alarms | Alarm Summary Dashboard |
| Art. 20 | PDP.3.1 | Provide detailed breach reporting | Enterprise forensic report | Forensic Incident Report |
| Art. 20 | PDP.3.1 | Support regulatory notification | Detailed event logs (User, File, Destination, Time) | Regulatory-ready export |

## Cross-Border Data Transfer Controls

### PDPL Article 29 | NDMO Domain 9.13

Restrict the transfer of sensitive data outside the Kingdom with the egress filtering capabilities of Fortra DLP. Organizations can define rules to block, warn, or require justification when classified or personal data is sent to external domains or unauthorized destinations, ensuring sensitive data remains within approved infrastructure.

| PDPL ARTICLE | NDMO CONTROL | REGULATORY REQUIREMENT | FORTRA CAPABILITY | EVIDENCE / OUTPUT |
|---|---|---|---|---|
| Art. 29 | DC.2.1 | Restrict transfer outside KSA | Egress filtering policies | Domain Blocking Logs |
| Art. 29 | DC.2.1 | Control email to external domains | Email destination control rules | External Transmission Alerts |
| Art. 29 | DC.2.1 | Ensure the minimum necessary transfer | Justification prompt and logging | User Justification Audit Trail |

FORTRA

Fortra.com

**About Fortra**

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

 