Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***EPMwDC***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***Ontology-Based Regulatory Compliance Model for an AI-Powered Espionage Detection System***

Table of Contents

Research Report: Ontology-Based Regulatory Compliance Model for an AI-Powered Espionage Detection System

Deliverable for Prototype Development

Prepared by: Security Research Laboratory (L3CE), Mykolas Romeris University, Vilnius, Lithuania

Project: Implementation of Mission-Based Science and Innovation Programs (Project No. 02-002-P-0001)

---

1. Purpose and Scope of This Document

This document accompanies the delivery of a research report and compliance model for the purpose of prototype development. It provides the technical and regulatory context necessary to develop a working prototype of a monitor with integrated espionage-prevention and malicious-activity-detection capabilities, compliant with applicable personal data protection and cybersecurity requirements.

The underlying research has been published as an open-access, peer-reviewed article:

Sabaliauskaite G, Paskauskas RA, Bružė E, Matulytė R, Lavišius T. *Automated regulatory compliance for AI systems in the security domain: The case of dual-use deployment.* Open Research Europe, 2026, 6:83. DOI: https://doi.org/10.12688/openreseurope.23137.1

All ontology files, SPARQL queries, and interactive visualisations referenced in this document are openly available (CC-BY 4.0 / MIT licence) from:

- GitHub: https://github.com/SecOntologyLab/regulatory-compliance-ontology
- Zenodo (archival): https://doi.org/10.5281/zenodo.18763491

---

2. What the Model Is

The delivered model is an ontology-based regulatory compliance framework implemented as a machine-readable knowledge graph in RDF/Turtle. It formalises the regulatory obligations that apply to an AI-powered espionage detection system across two deployment domains:

- Civilian use – corporate boardrooms, government offices, financial institutions, healthcare facilities.
- Defence use – NATO command centres, military briefing rooms, classified research facilities.

The framework enables a developer to:

1. *Query* which regulatory requirements apply to each system component in each deployment context.
2. *Validate* that system design and operational procedures satisfy the applicable legal obligations.
3. *Generate* deployment-specific compliance checklists from a single knowledge base.
4. *Trace* from individual system components to the specific legal provisions they must satisfy.

The model is *not* a legal opinion. It structures and makes retrievable the compliance obligations that legal experts have identified; it does not substitute for legal advice on their interpretation.

---

3. System Architecture

The espionage detection system comprises the following components:

Component	Function
Monitor	Displays sensitive or classified information
Camera (USB-connected)	Visual monitoring of the room
AI Detection Module (Ethernet-connected to monitor)	Analyses video feed to detect unauthorised photography attempts (e.g., camera lenses or smartphone screens pointed at the display)
5G Network Link	Transmits alert notifications to the remote monitoring station
Remote Monitoring Station	Receives alerts; stores captured images; enables security personnel access
Dedicated Security Personnel	Receive alerts and take appropriate response actions

3.1 Operational Workflow

The system operates in three phases:

1. *Detect.* The camera monitors the room. The AI module analyses the video feed to identify attempts at unauthorised picture-taking.
2. *Notify.* Upon detection, the system transmits an alert to the remote monitoring station. The alert includes: captured image (potentially containing faces), AI confidence level, timestamp, information about what was displayed on screen, and the monitor's location data.
3. *Act.* Security personnel at the remote monitoring station review the alert and take appropriate action.

Critical design note: The system does *not* perform biometric identification, categorisation, or profiling of individuals. It detects behavioural indicators (e.g., a camera lens directed toward a protected display) without associating detected persons with identifiable biometric templates. This functional scope is significant for regulatory classification under the EU AI Act.

4. The Ontological Framework

4.1 Design Methodology

The ontology was developed using a six-step methodology:

Step	Focus	Key Output
1	Problem Framing & Regulatory Scoping	Regulatory scope document
2	Conceptual Framework Development	Visual model and structural template
3	Ontology Design & Implementation	RDF/Turtle ontology file
4	Domain-Specific Requirements Population	Populated civilian and defence modules
5	Knowledge Graph Deployment	Deployed, navigable knowledge graph
6	SPARQL-Based Validation & Analysis	Validated results and query library

4.2 Ontology Structure

The ontology uses the namespace rc: <http://l3ce.lt/ontology/regulatory-compliance> and defines the following core elements:

Class Hierarchy:

- RegulatoryCompliance (root)
  - RegComplyforCivilUse
  - RegComplyforDefenceUse
- RegulatoryFramework
  - EURegulations → GDPR, NIS2Directive, EUAIAct, CyberResilienceAct
  - NATORegulations → NATOSecurityPolicy, NIAP, NATOCyberDefencePolicy, TEMPESTStandard
  - NatLawsAndRegs → national transposition laws
- LifecyclePhase → DesignAndDevelopment, UsageAndMaintenance
- DesignPrinciple → PrivacyByDesign, SecurityByDesign
- RequirementCategory → PrivacyRelated, SecurityRelated
- Requirement → individual compliance obligations

Key Object Properties:

Property	Connects	Purpose
hasPhase	Compliance domain → lifecycle phases	Allocates obligations to pre- or post-deployment
hasRequirement	Phases → specific requirements	Links lifecycle stages to compliance obligations
derivedFrom	Requirements → source regulations	Traceability to legal instruments
hasRequirementCategory	Requirements → privacy/security	Classifies the nature of each obligation
appliesToDomain	Requirements → civilian/defence	Enables deployment-specific filtering
hasDefenceEquivalent / hasCivilianEquivalent	Requirement → requirement	Maps cross-domain relationships

Key Datatype Properties:

Property	Example Value	Purpose
requirementIdentifier	"CIV-DESIGN-R1"	Unique structured identifier
articleReference	"GDPR Article 25, Article 35"	Citation to specific legal provisions
legalBasis	*(substantive text)*	Description of the compliance obligation

4.3 Accessing and Querying the Ontology

The RDF/Turtle file can be loaded into any standards-compliant triplestore (e.g., Stardog, GraphDB, Apache Jena Fuseki). Once loaded, SPARQL queries can retrieve deployment-specific requirements. For example:

Retrieve all civilian requirements:

```
PREFIX rc: <http://l3ce.lt/ontology/regulatory-compliance>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema>
SELECT ?identifier ?label ?category ?article ?legalBasis
WHERE {
 ?req a rc:Requirement ;
    rdfs:label ?label ;
    rc:requirementIdentifier ?identifier ;
    rc:hasRequirementCategory ?category ;
    rc:appliesToDomain rc:CivilianDomain .
 OPTIONAL { ?req rc:articleReference ?article }
 OPTIONAL { ?req rc:legalBasis ?legalBasis }
}
ORDER BY ?identifier
```

A complete SPARQL query library is included in the GitHub repository.

5. Regulatory Requirements Captured by the Model

5.1 Civilian Domain

Req. ID	Requirement	Category	Regulatory Source
CIV-DESIGN-R1	DPIA and Privacy by Design	Privacy-related	GDPR Article 25 (data protection by design), Article 35 (DPIA)
CIV-DESIGN-R2	Security Architecture by Design	Security-related	GDPR Article 32 (security of processing), NIS2 Article 21 (cybersecurity risk management)
CIV-USAGE-R3	Breach Notification and Data Subject Rights	Privacy-related	GDPR Article 33 (notification to supervisory authority), Article 34 (communication to data subject)
CIV-USAGE-R4	Operational Cybersecurity Measures	Security-related	NIS2 Article 21, GDPR Article 32

CIV-DESIGN-R1 – A Data Protection Impact Assessment is required before deployment. Data minimisation principles must govern image capture design: lens detection must avoid unnecessary recording and capture only what is essential for security verification. Retention periods must be defined during the design phase. The system architecture must embed privacy safeguards from inception.

CIV-DESIGN-R2 – Encryption architecture must be designed into the system from inception. Secure communication protocols are required for data transmission to the remote monitoring station. Hardened firmware and secure boot mechanisms must be specified during development. Access control frameworks must be architected before deployment.

CIV-USAGE-R3 – Personal data breaches must be reported to the supervisory authority within 72 hours. High-risk breaches require communication to affected data subjects without undue delay. The system must support data subject rights (access, erasure, restriction). Transparency notices are required in deployment locations.

CIV-USAGE-R4 – Encrypted data transmission required for all communications to the remote monitoring server. Access controls must restrict image viewing to authorised personnel only. Comprehensive audit logging of all system access and data processing activities. Incident response procedures must be documented and tested. Vulnerability management and regular security assessments are required.

5.2 Defence Domain

Req. ID	Requirement	Category	Regulatory Source
DEF-DESIGN-R1	DPIA and Privacy by Design	Privacy-related	National law (e.g., Lithuanian Law on Legal Protection of Personal Data for National Security/Defence), Article 25, Article 18
DEF-DESIGN-R2	NATO Security Controls	Security-related	NATO Information Assurance Policy (NIAP), NATO Security Policy (NSP)
DEF-USAGE-R4	NATO Cyber Defence Compliance	Security-related	NATO Cyber Defence Policy

DEF-USAGE-R4 decomposes into sub-requirements:

Sub-Req. ID	Sub-Requirement	Article Reference
DEF-USAGE-R4-ART3	Detection Mechanisms	Article 3, Paragraph 2
DEF-USAGE-R4-ART5	Secure Incident Reporting	Article 5, Paragraph 8
DEF-USAGE-R4-ART7	Threat Intelligence Sharing	Article 7, Paragraph 6

5.3 Key Compliance Principle: Defence Is Additive

For systems deployed in both civilian and defence domains, defence compliance does not replace civilian obligations – it adds to them. A system deployed in a NATO facility must comply with national data protection law, all applicable NIS2 requirements (as a civilian baseline), and NATO-specific requirements (NIAP, NSP, Cyber Defence Policy, and potentially TEMPEST certification for electromagnetic emissions security).

6. Component-to-Requirement Mapping

The following table maps each system component and its data/activity to the applicable requirements in each domain. This is the key reference for prototype developers to understand *which compliance obligations attach to which part of the system*.

System Component	Data/Activity	Civilian Requirements	Defence Requirements
USB Camera	Captures images of room occupants (potential personal data)	CIV-DESIGN-R1: DPIA required; data minimisation in image capture design	DEF-DESIGN-R1: DPIA required; privacy safeguards embedded in design
AI Detection Module	Processes visual data to identify unauthorised photography attempts	CIV-DESIGN-R2: Secure architecture; hardened firmware; secure boot	DEF-DESIGN-R2: NATO security controls; multi-layered access controls
Screen Interface	Ethernet connection; displays classified content	CIV-DESIGN-R2: Encryption architecture for data in transit	DEF-DESIGN-R2: NSP physical security

System Component	Data/Activity	Civilian Requirements	Defence Requirements
			requirements; TEMPEST considerations
5G Transmission	Transmits personal data (images, location) to remote server	CIV-USAGE-R4: Encrypted transmission; audit logging	DEF-USAGE-R4: Secure encrypted channels (Art. 5[8])
Remote Monitoring Station	Receives alerts; stores images; enables personnel access	CIV-USAGE-R3: Breach notification within 72 hours; data subject rights. CIV-USAGE-R4: Access controls; audit logging; vulnerability management	DEF-USAGE-R4-ART3: Detection and reporting mechanisms
Dedicated Personnel	View captured images; make response decisions	CIV-USAGE-R3: Transparency notices; purpose limitation	DEF-USAGE-R4-ART7: Threat intelligence sharing across NATO entities

7. Practical Guidance for Prototype Development

7.1 Single Platform, Dual Compliance Paths

The system should be developed as a single technical platform that supports configurable compliance paths depending on the deployment context:

Development Decision	Civilian Deployment	Defence Deployment
Encryption standard	Commercial TLS/AES (GDPR Art. 32, NIS2 Art. 21)	NATO-approved cryptographic modules
Access control	Role-based access with audit logging	Security clearance verification; need-to-know enforcement
Incident reporting	National supervisory authority (within 72 hours)	Secure encrypted channels to NATO entities
Data retention	Defined by DPIA; subject to erasure requests	May be extended for security evidence; erasure rights potentially limited
Certification	CE marking; NIS2 compliance attestation	TEMPEST certification; STANAG compliance

Recommendation: Design the system architecture to accommodate the more stringent defence requirements, enabling civilian deployment as a subset configuration.

7.2 Deployment-Specific Compliance Documentation

Documentation	Civilian Deployment	Defence Deployment
Regulatory basis	GDPR, NIS2 Directive	NIAP + NSP + NATO CDP
Applicable requirements	CIV-R1, CIV-R2, CIV-R3, CIV-R4	DEF-R1, DEF-R2, DEF-R4 (+ sub-requirements)

Documentation	Civilian Deployment	Defence Deployment
Certification evidence	NIS2 compliance; GDPR accountability documentation	TEMPEST certificate; NATO accreditation
Audit trail	Access logs; breach register; DPIA	Above + threat intelligence sharing records

7.3 Market Segments

Market Segment	Compliance Requirements	Supervisory Pathway
Corporate sector	GDPR, NIS2 (if critical infrastructure)	National authority registry control
Government (civilian)	GDPR, NIS2, national cybersecurity law	National authority accreditation
Financial institutions	GDPR, DORA	Regulatory compliance supervision
NATO/Defence	GDPR + full NATO framework	TEMPEST certification; NATO accreditation

8. Artefacts Provided

The following machine-readable artefacts are delivered alongside this document and are available from the repositories listed in Section 1:

1. *RDF/Turtle ontology file* – the complete regulatory compliance knowledge graph, loadable into any W3C-compliant triplestore.
2. *SPARQL query library* – pre-built queries for retrieving civilian requirements, defence requirements, cross-domain comparisons, sub-requirement decomposition, and component-to-requirement mappings.
3. Interactive D3.js visualisations – browser-based visual explorations of the ontology structure.
4. Methodology documentation – detailed description of the six-step methodology.

All files are in open, non-proprietary formats (Turtle/TTL, SPARQL, HTML) conforming to W3C Semantic Web standards.

9. Limitations and Future Extensions

The current ontology captures a representative subset of applicable regulations (GDPR, NIS2, NATO policies) with requirements specified at a summary level (R1–R4 per domain). For a production compliance system, the following extensions are anticipated:

- Full article-level coverage of GDPR, NIS2 Directive, and EU AI Act risk classification.
- Integration of the Cyber Resilience Act (CRA) and sector-specific frameworks (e.g., DORA for financial services).
- SHACL (Shapes Constraint Language) validation rules for automated checking of system specifications against regulatory constraints.
- Ontology versioning mechanisms to track regulatory evolution (e.g., CEN-CENELEC JTC 21 AI Act implementing standards as they are adopted).

Editor
<<Main Editor>>

Contributors
Evaldas Bruze (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Reviewers
Evaldas Bružė (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Disclaimer