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: ***OSOTS***

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

Action result: ***Analysis Report on Compliance with Cybersecurity Regulations and Regulatory Systems Inspection Report: OSOTS Project***

Analysis Report on Compliance with Cybersecurity Regulations and Regulatory Systems Inspection Report: OSOTS Project

Table of Contents

Introduction

The Open Source Operational Technology Sensor (OSOTS) project is designed to support cyber incident detection and response to maintain the integrity and reliability of industrial systems. Utilizing Machine Learning (ML) mechanisms, OSOTS provides real-time detection, intelligence, and alerts regarding anomalies in critical infrastructure sectors such as power plants, water distributors, and gas producers. Because OSOTS monitors network traffic and captures communication data, its lifecycle requires strict adherence to cybersecurity, data protection, and Artificial Intelligence (AI) regulations.

The result of the product will be open-source based network security monitoring software (sensor). Since the sensor is going to provide comprehensive monitoring of network traffic, allowing it to capture communication data and detect potential threats as well as devices connected to a network, it is important to ensure the projects' compliance with GDPR and cyber security regulations.

Therefore this Analysis Report on Compliance with Cybersecurity Regulations and Regulatory Systems Inspection Report provides a comprehensive information on the topic.

On the level of EU and NATO, while implementing this project, it is crucial not only to examine recent policy practices related to the implementation of the GDPR and AI in the field, but also to provide insights on the implementation of similar projects.

1. Main Phases of Implementation and Compliance

The implementation of the OSOTS system combines rigorous R&D milestones with compliance checkpoints built on the principles of "Security by Design" and "Dual-Use by Design".

- **Phase 1: Architectural Design & Risk Assessment:** This foundational stage focuses on translating legal requirements into code logic. It includes conducting a mandatory Data Protection Impact Assessment (DPIA) and defining the "Dual-Use" scope to serve both civilian and defense needs. To operationalize GDPR requirements into technical specifications, it is recommended to adopt the Standard Data Protection Model (SDM).

- **Phase 2: Data Processing & Model Training:** During the development of ML models, personal data and bias must be strictly managed. This involves implementing pseudonymization by default to ensure data unlinkability, detecting potential bias, and selecting interpretable ML algorithms to avoid opaque "black box" models.
- **Phase 3: Operational Deployment (Prototyping & Testing):** As the sensor actively monitors live network traffic, operators must configure the system for "targeted" data retention rather than general mass surveillance. The deployment must also implement a "Human-in-the-Loop" (HITL) workflow, ensuring the AI acts as a decision-support tool where human operators validate high-consequence alerts. R&D in this stage spans laboratory testing, adaptation to specific end-user environments, and end-user validation.
- **Phase 4: Incident Management & Response:** The post-detection phase focuses on integrating incident reporting capabilities. This includes generating data formats compatible with the NIS2 Directive for national Computer Security Incident Response Teams (CSIRTs) and utilizing NATO STANAGs to allow for cross-border intelligence sharing in the event of hybrid threats. Finally, the product will see commercial release under a dual-licensing (open-source and proprietary) model.

2. Most Important Aspects of Regulatory Compliance

Cybersecurity & Resilience (NIS2 and CRA)

- **Security by Design:** Compliance is architectural, not just administrative; under the Cyber Resilience Act (CRA), security must be integrated from the first design phase.
- **Incident Reporting:** The system must facilitate mandatory incident reporting and information sharing for critical entities as required by the transposed NIS2 Directive.

Data Protection & Privacy (GDPR)

- **Data Minimization:** The system must default to capturing only the "bare essentials," such as packet headers and metadata, rather than performing full packet content inspection unless strictly necessary.
- **Automated Decision-Making Restrictions:** Under GDPR Article 22 and the *SCHUFA* Court of Justice of the European Union (CJEU) ruling, if the sensor's risk score decisively influences

actions (such as blocking a user), it constitutes an automated decision and requires strict safeguards and human intervention.

- **Targeted Retention:** The *La Quadrature du Net* CJEU ruling prohibits the general and indiscriminate retention of traffic data unless there is a genuine and present threat to national security, meaning routine monitoring must rely on targeted retention.

AI Governance & Ethics (EU AI Act)

- **High-Risk System Oversight:** As a cyber threat management system for critical infrastructure, OSOTS is classified as a high-risk AI application.
- **Algorithmic Transparency:** Users maintain a "right to an explanation" under the *Dun & Bradstreet* ruling. Organizations must provide meaningful information about the "key parameters" that led to a specific alert or decision.
- **Accountability Principles:** The AI system's accountability is defined by 12 principles, including Lawfulness, Inclusivity, Transparency, Impartiality, Proof, Explainability, and Learning.

Defense & Dual-Use Frameworks

- **Interoperability:** The software must bridge civilian innovation and military needs, aligning with NATO's Emerging and Disruptive Technologies (EDTs) policy and Data Centric Reference Architecture to enable secure data sharing across alliances.

3. Practical Challenges

- **The "Black Box" vs. Transparency Paradox:** The legal requirement to explain the logic involved in automated decisions clashes with the operational reality that revealing source code or specific model weights could compromise the tool's effectiveness against cyber attackers or expose trade secrets.
- **Data Retention Boundaries:** It is challenging to navigate the legal line between "crime fighting" (where only targeted retention is allowed) and "hybrid threats" or national security crises (where mass retention is permitted). Operators may struggle to legally identify when they can activate full-capture modes without formal government declarations.

- **Defining Automated Decisions and Automation Bias:** If an AI sensor outputs a 99% risk score and overwhelmed human operators routinely follow it without deep investigation, it is legally ambiguous whether this constitutes a prohibited "automated decision" due to human automation bias.
- **Civilian vs. Defense Data Sharing:** Despite policies intended to bridge civil-defense gaps, decentralized national regulations create legal friction when a private civilian operator attempts to share un-anonymized threat data with military or intelligence units.
- **Deployment Costs and Complexity:** As seen with competitor solutions (Nozomi, Forescout, Dragos, Claroty), navigating the convergence of IT and OT environments involves managing high deployment friction, resource-intensity for smaller teams, and the risk of active querying techniques disrupting fragile industrial processes.

ANNEX 1: Implementation Stages Checklist

This checklist is structured around the four primary R&D and operational deployment stages of the OSOTS project.

Stage 1: Architectural Design & Risk Assessment

- **Conduct Data Protection Impact Assessment (DPIA):** Ensure a DPIA is executed immediately, as it is mandatory for AI systems monitoring public or private networks.
- **Define Dual-Use Scope:** Document and design the software architecture to serve both civilian critical infrastructure and military defense needs to qualify for relevant funding (e.g., European Defence Fund).
- **Apply the Standard Data Protection Model (SDM):** Translate abstract legal goals (such as integrity, transparency, and unlinkability) into concrete technical specifications within the sensor code.
- **Identify Legal Frameworks:** Identify all applicable laws, regulations, and policies for the deployment of the AI system, including legal exemptions and safeguards.
- **Integrate Security by Design:** Adopt a Secure Development Lifecycle (SDL) from the first design phase rather than treating security as an add-on.

Stage 2: Data Processing & Model Training

- **Enforce Data Minimization:** Restrict data capture to the bare essentials, such as packet headers and metadata, by default.
- **Implement Pseudonymization:** Establish pseudonymization domains so the entity analyzing the data cannot re-identify specific users without holding additional, separated information.
- **Document Data Sources:** Ensure the nature, source, and selection process for training, validation, and testing data are thoroughly documented.
- **Detect and Mitigate Bias:** Test for and prevent discriminatory outcomes in threat detection. If processing special data categories is required for bias detection, use legal exemptions and strict safeguards.

- **Avoid "Black Box" Models:** Select interpretable Machine Learning (ML) algorithms capable of providing meaningful information about the decision logic.

Stage 3: Operational Deployment (Prototyping & Testing)

- **Configure Targeted Retention:** Prevent general mass surveillance by configuring the system for targeted retention triggered only by specific geographic areas, timeframes, or threat indicators.
- **Implement Human-in-the-Loop (HITL):** Design the system as a Decision Support System; ensure human operators must review automated risk scores before significant actions (e.g., blocking a subnet) are executed.
- **Maintain Immutable Logs:** Maintain detailed logs to prove necessary security measures were active, which protects against liability in case of an incident.
- **Test in Target Environments:** Conduct laboratory testing and adapt the prototype to specific end-user environments by soliciting feedback and validating performance.

Stage 4: Incident Management & Response

- **Automate Incident Reporting:** Build features that format logs automatically for submission to national Computer Security Incident Response Teams (CSIRTs), complying with the NIS2 directive.
- **Adopt Standard Data Formats:** Ensure data output is compatible with cross-border intelligence-sharing formats, such as NATO STANAG 5636.
- **Establish Trust-Based Sharing:** Implement protocols that allow private operators to safely exchange un-anonymized threat data with supervisory authorities without risking trade secrets.

ANNEX 2: Regulatory & Functional Aspects Checklist

This checklist focuses on the overarching compliance domains that the OSOTS system must satisfy throughout its lifecycle.

1. Data Protection & Privacy (GDPR Focus)

- Is the processing of personal data necessary and proportionate to the security purpose?
- Are appropriate technical and organizational measures (e.g., encryption, pseudonymization) in place to integrate data protection?
- Are automated decisions that produce legal or significant effects prohibited unless strictly necessary and accompanied by human intervention options?
- Are there clear rules established on how data is collected, collated, shared, and retained?
- Are affected stakeholders informed about the data processing, and are there mechanisms in place to handle personal data breaches?

2. Artificial Intelligence Governance (AI Act & Accountability)

- Has the AI system been screened to ensure it does not use "prohibited practices" (e.g., manipulative techniques, social scoring)?
- If the AI model generates content, is it marked in a machine-readable manner?
- Is there algorithmic transparency allowing users the "right to an explanation" about the key parameters of flagged anomalies?
- Are the 12 Accountability Principles (e.g., Lawfulness, Inclusivity, Transparency, Explainability) formally documented and assigned to responsible actors?
- Are decisions made by the AI system documented and fully reversible?

3. Fundamental Rights & Stakeholder Impact (FRIA)

- Has a Fundamental Rights Impact Assessment (FRIA) been conducted for the deployment of this high-risk AI system?
- Are specific categories of natural persons or marginalized groups that might be affected by the system identified?

- Have all stakeholders who will use or be informed about the AI system been engaged?
- Are measures and internal governance arrangements in place to mitigate harms if identified risks materialize?
- Are oversight bodies identified, and are there procedures to allow affected stakeholders to complain or seek redress?

4. Cybersecurity, Resilience, and Dual-Use Standards

- Does the system comply with certification requirements under the Cyber Resilience Act (CRA)?
- Is the system capable of handling vulnerabilities safely across the software's entire lifespan?
- Have security boundaries and requirements (like IEC 62443 or NIST CSF) been verified?
- Can the system maintain its "dual-use" viability by bridging civilian infrastructure innovation and military strategic objectives without violating compliance?

Conclusions

The OSOTS project is highly relevant to current geopolitical priorities, addressing critical cybersecurity shortages through AI automation while aligning with the European Defence Industrial Strategy (EDIS) and NATO objectives. However, regulatory compliance for such a dual-use, high-risk system is inseparable from its underlying architecture. The most profound legal hurdles do not stem from data collection alone, but rather from the system's potential to automatically detect and block threats. Navigating these hurdles requires strict adherence to CJEU jurisprudence, ensuring that automated systems remain transparent and subordinate to human oversight.

Compliance with Cybersecurity Regulations

Compliance with cybersecurity regulations for the Open Source Operational Technology Sensor (OSOTS) project requires an architectural paradigm shift where legal mandates are hardcoded into the software's design, rather than treated as administrative add-ons.

- **Security by Design and Certification as a Foundation:** Under the Cyber Resilience Act (CRA) and the Union Rolling Work Programme, "Security by Design" is non-negotiable. The OSOTS sensor must secure data minimization from the very first design phase, defaulting to capturing only bare essentials like packet headers rather than full packet content. Securing a European cybersecurity certificate serves as a necessary "passport" that proves the software's resilience and smooths cross-border deployment across EU member states.
- **Mandatory Incident Reporting:** The transposition of the NIS2 Directive (as seen in national laws like Lithuania's Law on Cybersecurity) creates a legal mandate for operators of critical services to report incidents. OSOTS must be technically configured to facilitate this compliance by automatically formatting logs into reports required by national Computer Security Incident Response Teams (CSIRTs).
- **Balancing "Dual-Use" Data Sharing with Privacy Limitations:** The project operates as a dual-use technology aligning with the European Defence Industrial Strategy (EDIS) and NATO's

Data Centric Reference Architecture. It must use standard data formats (such as NATO STANAG 5636) to ensure cross-border intelligence sharing during hybrid threats. However, under the GDPR and CJEU jurisprudence (*La Quadrature du Net*), **general and indiscriminate retention of traffic data is strictly prohibited** unless there is a genuine, present threat to national security. Therefore, routine operations must be restricted to "targeted retention" based on specific risk indicators or geographic parameters.

- **Liability and Operational Logs:** Under the GDPR and the *Deutsche Wohnen* ruling, administrative fines are strictly tied to cases of "intent or negligence". To comply with overarching security protocols and defend against liability during unavoidable cyber incidents, the system must maintain immutable logs to prove that all necessary, state-of-the-art security measures were active.

Regulatory Systems Inspection

Regulatory inspection readiness for the OSOTS project revolves around verifiable accountability, algorithmic transparency, and the strict governance of automated decision-making. Supervisory authorities will scrutinize the system based on its ability to prove compliance, not just claim it.

- **Algorithmic Transparency and the "Black Box" Prohibition:** During an inspection, deployers must prove that their AI systems are not opaque "black boxes." Following the CJEU *Dun & Bradstreet* ruling, individuals and oversight bodies have a "right to an explanation". The system must be capable of providing **"meaningful information about the logic involved,"** explicitly outlining the key parameters that led the AI to flag an anomaly or make a decision. Even if the exact source code is protected as a trade secret, sufficient details must be generated to allow for external regulatory verification.
- **Mandatory Human-in-the-Loop (HITL) for Automated Decisions:** A critical focal point for any regulatory audit is Article 22 of the GDPR and its interpretation in the *SCHUFA* and *Ligue des droits humains* cases. If the OSOTS sensor generates a risk score that decisively influences an action, such as automatically blocking network access, it constitutes "automated individual decision-making". To pass inspection, **the system must be designed as a Decision Support System**, where human operators are required to review and validate any high-consequence alerts before actions are executed, thereby preventing the AI from acting as the sole arbiter.

- **Comprehensive Impact Assessments:** Regulatory authorities require documented proof of risk mitigation prior to deployment. The system deployer must be able to present a thoroughly documented Data Protection Impact Assessment (DPIA) and a Fundamental Rights Impact Assessment (FRIA). These assessments must clearly identify the risks of bias, list affected stakeholder groups, and establish the specific mechanisms in place to handle complaints or redress.
- **Evidence of Accountability Principles:** Inspections will heavily weigh whether the deployment follows established AI Accountability Principles, such as "Proof" (capturing reliable evidence mirroring law enforcement standards) and "Compellability" (oversight bodies must be able to access necessary information without external legal powers). Given that state audits (e.g., in Lithuania) have found a severe lack of AI risk mitigation procedures in the public sector, providing deployers with a bundled "compliance kit" containing verified templates and logs is essential to satisfying rigorous national inspection requirements.

Recommendations

- **Implement "Dual-Use by Design":** From the outset, develop the software architecture to serve both civilian and military objectives, which ensures eligibility for defense funding while remaining commercially viable for critical infrastructure.
- **Adopt the Standard Data Protection Model (SDM):** Utilize this methodology to translate abstract legal requirements, such as data minimization, integrity, and unlinkability, into concrete, verifiable technical configurations within the sensor code.
- **Mandate Human-in-the-Loop (HITL):** Design the dashboard as a Decision Support System. The AI should generate risk scores, but a human operator must validate any high-consequence actions (e.g., permanently blocking a subnet) to comply with CJEU rulings on automated decision-making.
- **Ensure Algorithmic Transparency:** Avoid fully opaque "black box" models. The system must be capable of generating intelligible explanations detailing the key parameters that flagged an anomaly, satisfying the legal right to explanation.

- **Conduct and Maintain DPIAs:** Ensure a Data Protection Impact Assessment is executed prior to deployment, specifically to assess the risks related to ML bias, automated decision-making, and public network monitoring.
- **Pursue European Cybersecurity Certification:** Prepare the software for certification under the Cyber Resilience Act (CRA) framework, which serves as a necessary passport for cross-border operations across EU member states.
- **Develop Trust-Based Sharing Protocols:** Build features that automatically format logs for national CSIRTs and facilitate safe data exchange between private enterprises and supervisory authorities without the fear of leaking proprietary data or violating the GDPR.

References

1. General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
2. CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
3. CJEU Case C-817/19 - Ligue des droits humains. https://curia.europa.eu/juris/liste.jsf?num=C-817/19
4. Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
5. CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
6. NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
7. Cyber Resilience Act. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847
8. Joint Comminication. European Defence Industrial Strategy (EDIS) (March 2024). https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=EDIS%20Joint%20Communication.pdf
9. Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies (EDTs) (February 2021). https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies
10. Union Rolling Work Programme for European cybersecurity certification. https://ec.europa.eu/newsroom/dae/redirection/document/102292
11. CJEU Case C-511/18 - La Quadrature du Net and Others, 2020. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
12. Guidelines on prohibited artificial intelligence (AI) practices. February 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act
13. The General-Purpose AI Code of Practice: https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
14. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr

15. Data Strategy for the Alliance (May 2025). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance
16. The Standard Data Protection Model. A method for Data Protection advising and controlling on the basis of uniform protection goals: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM_V3_en.pdf
17. Apply AI Strategy (COMMUNICATION FROM THE COMMISSION Artificial Intelligence for Europe) COM(2025) 723 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0723
18. CJEU Case C-807/21 - Deutsche Wohnen, 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=282192&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8123480
19. Cybersecurity Entity Register (CISE). https://www.nksc.lt/ksis
20. Finland's Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content
21. Sweden in a digital world. A strategy for Sweden's foreign and security policy on cyber and digital issues. https://www.government.se/contentassets/f858cec8cb944d3fa82bdf0fb7959448/sweden-in-a-digital-world---a-strategy-for-swedens-foreign-and-security-policy-on-cyber-and-digital-issues.pdf
22. Defence Readiness Omnibus. Simplification proposal to boost industrial readiness. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-readiness-omnibus_en

Editor
<<Main Editor>>

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

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