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: ***Modeling According to the Principles of Privacy by Design and Privacy by Default: Deployment Requirements***

Modeling According to the Principles of Privacy by Design and Privacy by Default: Deployment Requirements

Table of Contents

Introduction

The project “Research and development of an Espionage Prevention Monitor with Detection Capabilities (EPMwDC)” seeks to develop a unique product consisting of hardware and software modules, which would enable government and private organisations to prevent sensitive data leaks when a picture is taken of the screen, displaying confidential data, detecting and reporting to authorities if such incident is realised.

While the pre-deployment phases focus on engineering privacy and security into the system's architecture, the deployment and operational phase is where these technical safeguards are activated, governed, and legally operationalized by the end-user entity. Deployment according to "Privacy by Design" and "Privacy by Default" principles demands that the system's runtime environment, user workflows, and maintenance protocols continuously uphold data protection and cyber resilience.

Below is a detailed elaboration of the specific requirements, key stages, and critical aspects that must be taken into account during the deployment of a dual-use AI system.

1. Key Stages in the Deployment Phase

The deployment lifecycle ensures that the system transitions from a controlled development environment to a live operational setting without compromising its embedded security features.

Stage 1: Secure Installation, Configuration, and Integration

Deployment must follow strict security policies (such as the NATO Security Policy) to ensure secure installation and configuration. This stage involves phased rollouts and rigorous compatibility testing to integrate the system with the deployer's existing IT infrastructure, such as connecting a civilian system to corporate networks or integrating a defense system into classified, segmented networks (e.g., Lithuania's *Saugusis tinklas*).

Stage 2: Operational Training and Capacity Building

The deployment phase must include comprehensive training for the personnel who will operate and monitor the system. Operators must be proficient in reviewing system alerts, responding to incidents, and understanding their responsibilities regarding data protection and AI accountability.

Stage 3: Active Operation, Monitoring, and Incident Handling

During live operation, the system continuously monitors the designated environment (e.g., a workstation) and relies on configured thresholds to flag potential threats. The focus at this stage is on managing the generated evidence, executing access controls, and handling breach notifications.

Stage 4: Adaptability, Re-evaluation, and Updates

The deployment is not static. Operational use requires continuous vulnerability management, regular security assessments, and the deployment of necessary patches (e.g., over-the-air updates). Furthermore, operator feedback (such as marking false positives) must be structurally managed to improve the AI model over time.

2. Specific Deployment Requirements and Key Aspects

1. End-User/Deployer Accountability and Organizational Measures

While a system can be engineered with Privacy by Design, full compliance in a live environment depends heavily on the deployer's organizational measures.

- **Configuration of Default Settings:** The end-user entity is strictly responsible for configuring the system's parameters according to their internal policies and legal basis. This includes defining exact data retention periods, establishing the lists of prohibited objects, and tuning detection thresholds.
- **Internal Governance:** The deployer must establish clear internal governance, including assigning responsibilities for overseeing data processing, incident handling, and responding to data subject access requests (DSARs).

2. Operational Cybersecurity Measures

Post-deployment security relies on strict access management and continuous monitoring to protect the forensic data gathered by the system.

- **Encrypted Transmission and Access Control:** All operational communications to remote monitoring servers must utilize encrypted channels (e.g., TLS/AES for civilian use, or NATO-approved cryptographic modules for defense). Access to the remote server must enforce multi-factor authentication, and data viewing must be restricted strictly to authorized personnel.
- **Continuous Audit Logging:** The system must actively maintain immutable audit logs recording all system access, user actions, and data processing activities. These logs ensure full traceability and accountability during operational use, allowing security teams to reconstruct how an alert was handled.

3. Operationalizing Human Oversight (Human-in-the-Loop)

Deployment procedures must ensure that AI does not act autonomously in ways that produce legal or disciplinary effects on individuals.

- **Review Workflows:** The deployment workflow must insert a human operator (e.g., an analyst or security officer) to review all AI-generated alerts.
- **Reversible Outcomes:** The human operator must possess the final authority to assess whether an alert is justified, mark it as a false positive or negative, and override the AI's preliminary classification, ensuring that all machine decisions are fully reversible.

4. Dual Compliance Paths for Incident Reporting

Deployment requires an incident response plan tailored to the specific domain (Civilian vs. Defense), acknowledging that the regulatory burden is additive for dual-use technologies.

- **Civilian Deployment:** The deployer must have processes in place to report personal data breaches to national supervisory authorities within 72 hours, adhering to GDPR Article 33 and NIS2 reporting structures.
- **Defense Deployment:** Incidents must be reported through secure, encrypted channels directly to military or NATO entities. Furthermore, defense deployments require active threat intelligence sharing across allied networks to combat coordinated espionage attempts.

5. Transparency and Stakeholder Engagement

Even in high-security environments, the deployment of AI monitoring tools requires adherence to transparency principles, balanced against security needs.

- **Privacy Notices:** Organizations deploying the system must provide appropriate internal privacy notices to affected stakeholders (such as employees or contractors working at the monitored workstations). These notices must explain the system's purpose, the conditions under which data is captured, and the rights of the data subjects.

6. Dynamic Updating of Impact Assessments (DPIA & FRIA)

Impact assessments are not merely pre-deployment hurdles; they are living documents during the operational phase.

- **Contextual Triggers for Re-evaluation:** The Data Protection Impact Assessment (DPIA) and the Fundamental Rights Impact Assessment (FRIA) must be actively updated by the deployer whenever the operational context changes. Material changes that necessitate an update include modifications to the deployment scope, changes in data flows, shifts in the physical environment being monitored, or alterations to the categories of affected persons.

Annexes: Deployment Requirements (Operationalizing Privacy and Security)

Annex 1. Key Stages in Deployment

Key Stages in Deployment	
Secure Installation and Configuration	• Integrating the system into the deployer's specific environment (e.g., civilian corporate networks or secure military infrastructure) following strict security policies.
Operational Training	• Providing extensive capacity-building for personnel to ensure they are proficient in managing the system, reviewing alerts, and understanding data protection rules.
Active Operation and Incident Handling	• Continuously monitoring the designated zone, managing generated evidence, enforcing role-based access, and securely reporting positive threats.
Adaptability and Assessment Re-evaluation	• Updating the DPIA and FRIA dynamically whenever the operational context, physical environment, or scope of monitored persons changes.

Annex 2. Compliance Checklist

Compliance Checklist	**[ ]**	• Establish the legal basis for processing (e.g., GDPR Art. 6(1)(e) or 6(1)(f)) and configure deployment-specific internal data governance.
	[ ]	• Configure exact data retention periods within the system, aligned with the deployer's internal policies, ensuring automated deletion.
	[ ]	• Deploy Transparent Privacy Notices to inform affected stakeholders (e.g., employees) about the scope and purpose of the monitoring.
	[ ]	• Ensure a strictly enforced "Human-in-the-Loop" workflow where all automated AI alerts are subject to human review and are fully reversible.
	[ ]	• Establish secure incident response and breach notification protocols (e.g., within 72 hours for civilian authorities).

Annex 3. Challenge Overcoming

Challenges	Suggestions to Overcome Challenges
• **Disproportionate Deployment and Mass Surveillance:** End-users might attempt to use the system for general, continuous employee monitoring rather than specific threat detection, risking violation of CJEU precedents (*La Quadrature du Net*) prohibiting blanket mass surveillance.	• **Enforce Configuration Safeguards:** Design the system interface to default to privacy-preserving settings (Privacy by Default), focusing purely on localized threat detection rather than continuous recording.
• **Fragmented Incident Reporting:** Adhering to strict, sometimes conflicting, reporting timelines (e.g., 24-hour early warnings for Lithuania's KSIS vs. 72-hour GDPR breach rules).	• **Automated Integration with Reporting Platforms:** Build API connectors linking the system directly to national reporting platforms (like the NKSC) to help clients efficiently meet tight regulatory deadlines.
• **Human Error and Misuse:** The effectiveness of the deployment is highly vulnerable to operator error, such as misclassifying false positives, failing to conduct proper investigations, or failing to maintain the integrity of evidence.	• **Comprehensive Training and Immutable Logging:** Mitigate human error by mandating operational training for security personnel and ensuring the system maintains immutable audit logs of all human decisions and interactions.

References

1. Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
2. 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
3. The Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847
4. Digital Operational Resilience Act: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
5. General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
6. NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
7. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
8. NATO AI Strategy, 2024. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy
9. Treaty on European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT
10. CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
11. Data Strategy for the Alliance, 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance
12. NATO's Data and Artificial Intelligence Review Board, 2022: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/natos-data-and-artificial-intelligence-review-board
13. CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
14. NATO Digital Backbone, 2024: https://www.nato.int/en/news-and-events/articles/news/2024/12/13/nato-digital-backbone
15. White Paper on Export Controls COM(2024) 25 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025
16. Dual-Use Regulation (2021/821): https://eur-lex.europa.eu/eli/reg/2021/821/2024-11-08/eng
17. European Commission. AI Act Single Information Platform: https://ai-act-service-desk.ec.europa.eu/en
18. Action Plan on synergies between civil, defence and space industries. COM(2021) 70 final. https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/action-plan-synergies-between-civil-defence-and-space-industries

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