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: ***EPMwDC Case, Comparative, and Content analysis***

EPMwDC Case, Comparative, and Content analysis

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.

Currently, the market does not offer similar solutions, making this a world-new innovation and addressing the unsolved problem.

This document provides a comprehensive case, comparative, and content analysis regarding implementation aspects related to EPMwDC implementation, taking into account privacy and cybersecurity aspects.

The case analysis involves examining real-world cases to gain insights into the implementation of similar projects. This approach can provide valuable information on how GDPR, AI Act and cybersecurity principles have been applied in practice and what challenges or limitations may exist.

The comparative analysis involves comparing and contrasting different approaches to privacy and security legal issues, also in order to identify best practices or areas for improvement.

Content analysis includes recent policy initiatives and implementing documents related to the project's issues in artificial intelligence, data protection and other aspects. The uniqueness of the project lies in the areas of activity covering the dual-use domain, therefore, when assessing recent policy initiatives within the scope of the project, certain measures may apply only to the civilian domain, and some to the dual-use or exclusively defense domain.

1. Case Analysis

Any technology of this nature must not only meet high-level technical standards, but also meet the requirements of the legal environment in which it will operate. Analysis of the regulatory environment and analysis of key policy practices in the EU and NATO contexts shows that this and all similar technologies must overcome certain regulatory and practical legal application challenges. Such challenges may manifest themselves in the form of legal uncertainty (non-specificity), especially in such complex and complex areas as data protection, the security of artificial intelligence technologies and the domain of dual-use technologies.

The goal of such case analysis involves examining real-world cases to gain insights into the implementation of privacy by design and security by design principles. This approach can provide valuable information on how these principles have been applied in practice and what challenges or limitations may exist.

However, currently, the market does not offer similar solutions, making this a world-new innovation and addressing the unsolved problem. Therefore, the scope of this case analysis involves not only real-world scenario but also a hypothetical scenario of the project implementation issues, related to the uncertainty of the regulatory environment, uncertainty in the broader field of activity: in the domain of social, hybrid, informational, cyber threat intelligence platforms with aspects of the dual-use area.

It has to be noted that some companies that offer counter-espionage services include Kroll, Berkeley Research Group, and Black Cube. However, specific information on their success stories in detecting reflections in glass and lenses may not be publicly available. A hypothetical case analysis is intended for such cases, so that the inaccessibility of information managed by private commercial entities does not prevent the study of practical implications.

1.1. Regulatory approach and operational *modus vivendi* in hypothetical scenarios

The regulatory approach in the case of the implementation of the technology discussed above includes several levels, assuming that the technology will be implemented in the Euro-Atlantic legal space:

1. EU legal regulatory domain;
2. NATO legal regulatory domain;
3. Legal domain of individual member states.

1.1.1. The "Dual-Use" Regulatory Problem

The EPMwDC project operates in a complex "omni-use" or dual-use environment. While the product addresses a gap in espionage prevention, it faces a bifurcated legal landscape. The EU AI Act[1] applies strictly to any dual-use system that enters the civilian market (e.g., banking, private enterprise), while NATO policies and national defense laws govern its use in purely military contexts. Relying solely on a "national security" exemption to bypass EU regulations is risky, as the CJEU has ruled[2] that such exemptions must be temporary and specifically justified, prohibiting blanket mass surveillance.

1.1.2. Mandatory "By Design" Requirements

Both EU and NATO frameworks demand that security and ethics be engineered into the product from the start, not added as an afterthought. EU Context: The Cyber Resilience Act[3] and NIS2 Directive[4] (transposed in Lithuania)[5] require strict cybersecurity standards for hardware and software products. NATO Context: The Alliance mandates "Security by Design" and alignment with the Principles of Responsible Use (PRUs)[6], specifically regarding reliability, governability, and bias mitigation.

1.1.3. The intertwining of individual states and supranational regulation

It has to be stressed that the legal domain of individual Member States can significantly affect the implementation of the project through three primary mechanisms: the interpretation of "National Security" exemptions, the specific transposition of EU directives (like NIS2), and divergent procedural laws regarding liability and surveillance.

- ***The "National Security" Exemption and Jurisdiction*** – The most critical factor is how individual Member States interpret the boundary between civilian and national security competences. Under Article 4(2) of the Treaty on European Union[7], national security remains the sole responsibility of each Member State. Consequently, the EU AI Act explicitly excludes AI systems developed or used *exclusively* for military, defense, or national security purposes from its scope.
- ***Fragmentation of Liability and Procedural Law*** – While the EU AI Act aims to harmonize rules, the legal landscape for liability and enforcement remains fragmented across Member States.
- ***National Transposition of Directives (The "Gold-Plating" Effect)*** – EU Directives require transposition into national law, allowing Member States to impose stricter or more specific requirements ("gold-plating").
- ***Divergent Administrative Governance*** – The practical application of the AI Act relies on national competent authorities: supervisory bodies, regulatory sandboxes, etc.

1.2. Practical implications for the hypothetical Case Analysis

Practical implications for the hypothetical case analysis heavily rely on already mentioned intersection of EU / NATO regulatory domain and legal domain of individual member states. The analysis uses a hypothetical

[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] NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
[5] Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
[6] 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
[7] Treaty on European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT

case study to illustrate the specific steps, legal obligations, and challenges involved in a dual-use context (Civilian vs. Defense).

Hypothetical Case Study: "EPMwDC"

Scenario: A Lithuanian deep-tech startup is developing the EPMwDC, which is a hardware/software solution that uses computer vision to detect cameras pointing at screens to prevent data leakage. They intend to sell two versions:

1. **EPM-Civ:** For commercial banks to protect client data.
2. **EPM-Mil:** For the Ministry of National Defence (MND) and NATO allies to protect classified intelligence.

1.2.1. The Compliance Checklist

This checklist differentiates between the civilian (EU Law) and military (National/NATO Policy) obligations, which shows the complexity of the compliance issue whithin the dual-use domain.

A. Civilian Market (EPM-Civ)

- **Classification:** Determine if the system is "High-Risk" under the EU AI Act. Since it involves biometrics (if detecting faces) or critical infrastructure protection, it likely qualifies.
- **Fundamental Rights Impact Assessment (FRIA):** Required for high-risk deployers to assess impact on employee privacy.
- **GDPR Compliance:**
  - **Data Protection Impact Assessment (DPIA):** Mandatory for systematic monitoring of employees (GDPR Art. 35).
  - **Automated Decision-Making:** Compliance with GDPR Art. 22 if the system automatically locks user accounts without human review.
  - **Right to Explanation:** Must explain the "logic involved" in detection to affected users (CJEU *Dun & Bradstreet* ruling)[8].
- **Cybersecurity:** Compliance with NIS2 Directive (transposed in Lithuania) for reporting incidents and Cyber Resilience Act for hardware security.

B. Defense Market (EPM-Mil)

- **AI Act Exemption:** Invoke Article 2(3) of the AI Act for systems used *exclusively* for military/national security purposes.
- **NATO Ethics Alignment:** Verify compliance with NATO's 6 Principles of Responsible Use (PRUs): Lawfulness, Responsibility, Explainability, Reliability, Governability, Bias Mitigation.
- **Data Interoperability:** Ensure adherence to STANAG 5636 standards[9] for semantic interoperability within the Alliance.
- **Supply Chain Security:** Verify "Security by Design" to prevent adversarial AI attacks (Data Poisoning).

1.2.2. Most Important Implementation Stages

According to the previous analysis of the EU / NATO regulatory requirements and policy practices, four critical stages for a dual-use lifecycle:

[8] CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
[9] 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

1. **Strategic Segmentation (Design Phase):** Separating the product lines to avoid the "Dual-Use Regulatory Trap".
2. **Data Governance & Training:** Handling the data used to teach the AI to recognize cameras/screens.
3. **Testing & Validation:** Proving the system works without bias or vulnerabilities.
4. **Operational Deployment:** The actual installation and monitoring phase.

Stage 1: Strategic Segmentation (Design Phase)

- **Step 1 (Civil):** Integrate "Privacy by Design." The camera feed should be processed locally (Edge AI) and discarded immediately, storing only metadata of the incident (time/location) to minimize GDPR exposure.
- **Step 2 (Defense):** For EPM-Mil, the company should engage with the EU Observatory of Critical Technologies to align with defense capability needs.
- **Step 3 (Legal):** Clearly define the "Intended Purpose" in the technical documentation. If EPM-Civ is marketed as "dual-use" for police, it triggers the full AI Act. If EPM-Mil is "exclusively" for the MND, it falls under national laws.

Stage 2: Data Governance & Training

- **Step 1 (Data Sources):** Use high-quality, unbiased datasets. Data Labs associated with AI Factories should be used to access secure, high-quality training data.
- **Step 2 (NATO Alignment):** Create a "DARB-Ready File" (Data and AI Review Board)[10]. This "Responsibility Folder" documents data provenance to prove the system isn't trained on compromised data from adversarial states.
- **Step 3 (Bias Mitigation):** Ensure the computer vision doesn't misidentify certain skin tones or behaviors as "espionage threats" more often than others, complying with both GDPR fairness principles and NATO's "Bias Mitigation" PRU.

Stage 3: Testing & Validation

- **Step 1 (Sandboxing):** For EPM-Civ: Apply to the AI Act Regulatory Sandbox (operational by 2026) to test compliance without fear of immediate fines. For EPM-Mil: Apply to NATO DIANA (Defence Innovation Accelerator). This allows testing in "denied environments" (e.g., jamming scenarios).
- **Step 2 (Adversarial Testing):** Conduct "Red Teaming" to see if the AI can be tricked (e.g., by holding a phone at a specific angle). This satisfies the "Robustness" requirement of the AI Act (Art. 15) and NATO's "Reliability" principle.
- **Step 3 (Hardware Security):** Ensure the hardware module meets Cyber Resilience Act standards (e.g., secure boot, encrypted updates) to prevent the EPM itself from becoming a listening device.

Stage 4: Deployment & Operations

- **Step 1 (Human Oversight):** Implement "Human-in-the-Loop" protocols. If system detects a camera, it should flag the user for a security officer to review, rather than automatically firing/locking them out. This avoids liability under the Schufa and Ligue des droits humains CJEU[11] rulings.

[10] 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
[11] CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21

- **Step 2 (Incident Reporting):** Civil: Connect to the NIS2 reporting structure (Lithuanian National Cybersecurity Center) for significant cyber incidents. Defense: Utilize the NATO Digital Backbone[12] for interoperability with allied command structures.

1.2.3. Practical Challenges – Lack of Legal Clarity

A. The "Omni-Use" Trap and Export Control

- **Challenge:** the hypothetical company creates one core algorithm. If they export EPM-Civ to a non-EU country, does it require a military export license because the algorithm is identical to EPM-Mil?
- **Context:** the White Paper on Export Controls[13] suggests bridging civil and defense R&D, but current regulations are fragmented. The AI Act applies to dual-use items on the civilian market, potentially creating conflicting documentation requirements with the Dual-Use Regulation (2021/821)[14].

B. The "National Security" Boundary

- **Challenge:** The Lithuanian MND might deploy EPM-Mil for "hybrid threat" monitoring (e.g., protecting energy grids).
- **Context:** The CJEU (La Quadrature du Net) ruled that "National Security" is not a blank check. If the threat isn't "genuine and present," blanket surveillance is illegal. It is unclear if detecting screen photos counts as "general and indiscriminate" surveillance if deployed broadly across government offices.

C. "Black Box" Liability vs. Security

- **Challenge:** A user accused of espionage by EPM-Civ demands an explanation (GDPR Art. 15). The company claims the AI logic is a "Trade Secret" or a "Security Feature" (revealing how it detects cameras allows users to bypass it).
- **Context:** The Dun & Bradstreet ruling states trade secrets cannot justify a refusal to explain the logic. There is a lack of clarity on how to explain the AI's decision without revealing vulnerabilities that spies could exploit.

D. Fragmentation of Support

- **Challenge**: The startup needs funding. InvestAI targets "AI Gigafactories", and NATO NIF targets defense.
- **Context**: Navigating between the AI Act Service Desk[15] (for compliance) and DIANA (for defense innovation) requires managing two distinct bureaucratic languages, despite the technology being identical. The Action Plan on Synergies[16] encourages cross-fertilization, but practical funding streams often remain siloed.

[12] NATO Digital Backbone, 2024: https://www.nato.int/en/news-and-events/articles/news/2024/12/13/nato-digital-backbone
[13] White Paper on Export Controls COM(2024) 25 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025
[14] Dual-Use Regulation (2021/821): https://eur-lex.europa.eu/eli/reg/2021/821/2024-11-08/eng
[15] European Commission. AI Act Single Information Platform: https://ai-act-service-desk.ec.europa.eu/en
[16] 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

1.3. Real-world case analysis

Already mentioned that some companies that offer counter-espionage services provide similar but not identical products on the market. Moreover, specific information on their success stories in detecting reflections in glass and lenses may not be publicly available. Therefore, this section only analyses publicly available information, including a summary of assessments conducted by other entities and other practical insights relevant to the context of this project. In this way, it is a descriptive analysis that reveals the main aspects of the functioning of certain real-world examples.

1.3.1. Kroll: The Institutional Defense Model

Kroll operates under a framework of Enterprise Security Risk Management (ESRM), focusing on the convergence of physical and digital threats. Their approach is defensive and institutional, aligning closely with corporate governance standards[17].

- **Proactive Adherence:** Kroll emphasizes strict adherence to regulatory frameworks. In their investigations, they actively assess whether data breaches trigger GDPR reporting requirements or notifications to Information Commissioners. For example, in an insider threat case, Kroll utilized digital forensics to confirm that no PII was stolen, specifically to resolve regulatory liability concerns.
- **Ethical Standards:** They operate under a formal "Code of Conduct and Business Ethics" and adhere to the "12 Basic Principles of Internal Investigations," which prioritize fairness, objectivity, and the protection of confidentiality to avoid liability and retaliation.
- **Technical Implementation (TSCM & Forensics):**
    - **Technical Surveillance Countermeasures (TSCM):** Kroll employs advanced detection hardware, including spectrum analyzers and non-linear junction detectors, to sweep for audio/video devices in boardrooms and executive suites. They emphasize a "proactive" approach, moving from reactive sweeps to continuous monitoring.
    - **Cyber-Physical Convergence:** Kroll addresses the "digital footprint" risk, noting that hacking geolocation data (as seen in the Gravy Analytics breach) renders physical security vulnerable without the need for physical bugs. They integrate cyber threat intelligence with physical security assessments to mitigate these hybrid threats.
- **Challenges & Risks: Insider Threats –** Kroll identifies trusted employees as a primary vector for espionage. The challenge lies in balancing employee trust with the necessary controls to prevent IP theft and financial fraud.

1.3.2. Berkeley Research Group (BRG): The Forensic & Regulatory Model

BRG combines academic rigor with forensic accounting, focusing heavily on high-stakes litigation, economic regulation, and compliance[18].

- **Compliance & Legal Framework (ISO/FCPA):**
    - **Certifiable Standards:** BRG strongly aligns with international standards, specifically assisting clients in attaining ISO 37001 certification (Anti-Bribery Management Systems).
    - **Regulatory Consulting:** Their practice is deeply rooted in compliance with the Foreign Corrupt Practices Act (FCPA) and Anti-Money Laundering (AML) regulations. They act as

[17] The most of the information about "Kroll" is retrieved from the official Krol, LLC website: https://www.kroll.com/en/about-us

[18] The most of the information about "BRG" is is retrieved from the official Berkeley Research Group, LLC website: https://www.thinkbrg.com/

independent auditors and monitors for government agencies, positioning themselves as objective third parties in legal disputes.

- **Technical Implementation (eDiscovery & Data):**
  - **Electronic Discovery:** BRG utilizes advanced data analytics to manage the "volume, variety, and velocity" of Electronically Stored Information (ESI). Their implementation involves forensic collection from cloud providers, mobile devices, and corporate networks to detect fraud and trade secret theft.
  - **Cybersecurity:** They deploy endpoint detection monitoring and stricter access controls as part of their remediation strategies following incidents.
- **Challenges & Risks:** Data Custodianship Risks – BRG itself became a target in 2025 when a ransomware attack compromised sensitive client data (SSNs, medical info, financial data) held on their systems. This highlights the high risk faced by firms that aggregate sensitive intelligence, requiring them to implement the very "Security by Design" principles they advise clients on.

1.3.3. Black Cube: The Tactical & Offensive Model

Black Cube represents the "dual-use" dilemma in the private sector. Staffed by former Israeli intelligence officers (Mossad/IDF), they apply military-grade HUMINT (Human Intelligence) tactics to commercial disputes[19].

- **Compliance & Legal Framework (The "Dual-Use" Gap):**
  - **Legal vs. Ethical:** While Black Cube asserts that its operations are supported by "expert legal opinions" and comply with local laws, they operate in a gray area that often challenges ethical frameworks. Their methods have led to significant controversies, including convictions of employees in Romania for harassment and hacking.
  - **Contrast with EU Standards:** Unlike the transparency mandated by the EU AI Act or GDPR, Black Cube relies on "complex cover stories" and deception. Their operations often aim to extract information through social engineering rather than protecting data privacy.
- **Technical Implementation (HUMINT & Social Engineering):**
  - **Offensive Social Engineering:** Unlike Kroll, which trains clients against social engineering, Black Cube utilizes it as a primary tool. They create fake companies and personas to elicit information from targets (e.g., the Harvey Weinstein case).
  - **Operational Scope:** Their implementation involves "deep covert operations" and establishing physical bases of operation (e.g., renting hotel floors) to gather intelligence on political or corporate opponents.
- **Challenges & Risks:**
  - **Reputational & Legal Liability:** The firm faces high risks of "blowback." Their aggressive tactics have resulted in lawsuits (e.g., defamation suits in Canada) and criminal probes.
  - **Adversarial Use of Technology:** Black Cube exemplifies the "adversarial" threat profile that defensive measures (like the EPM project) are designed to detect, specifically the use of recording devices and espionage tactics in non-public environments.

1.3.4. Summary

In the context of the dual-use domain (civil and defense):

- **Kroll** and **BRG** align with civilian defensive standards (GDPR, ISO 37001, NIS2), functioning as "protectors" that implement security by design to safeguard critical infrastructure and proprietary data.

[19] The most of the information about "Black Cube" is is retrieved from the official B.C. Strategy, Ltd website: https://www.blackcube.com/

- **Black Cube** operates closer to the military/intelligence offensive model, applying state-level espionage tradecraft to the private sector. This places them in the exact risk category that regulations like the EU AI Act (prohibiting manipulative practices) and NATO's "Responsible Use" principles seek to govern or mitigate against.

2. Comparative Analysis

Analysis of the regulatory environment and analysis of key policy practices in the EU and NATO contexts shows that this and all similar technologies must overcome certain regulatory and practical legal application challenges. Since the legal regulation of the area in question includes a number of strict rules, this comparative analysis aims to reveal possible different implementation scenarios and opportunities within the existing legal framework in particular jurisdictions.

This comparative analysis involves comparing and contrasting different approaches to privacy by design and security by design principles in order to identify best practices or areas for improvement.

Comparative analysis evaluates the regulatory environment and implementation scenarios for the EPMwDC project. The analysis distinguishes between the Civilian Scenario (commercial banks, critical infrastructure) and the Defense/Military Scenario (NATO, Ministries of Defence), drawing on the legal texts and case studies.

2.1. Comparative analysis of different legal approaches within the EU legal framework

2.1.1. Analysis of the Regulatory Environment

The EU regulatory environment for EPMwDC is characterised by a transition from voluntary guidelines to binding, risk-based legislation. The framework creates a "safety net" for civilian applications while acknowledging a distinct operational reality for national security.

The "Safety Net" (Civilian): The AI Act (Regulation 2024/1689)[20] is the central pillar. It classifies AI based on risk. EPMwDC, involving computer vision and potential biometric data (identifying a person holding a camera), likely falls under High-Risk AI Systems (Annex III), specifically regarding critical infrastructure management or employment/workers management. This triggers mandatory conformity assessments, data governance, and logging requirements.

Operational Resilience: The NIS2 Directive (2022/2555)[21] and DORA (2022/2554)[22] mandate that entities (like banks or energy grids) using EPMwDC must ensure the security of the network and information systems themselves.

The Defense Exemption: The AI Act explicitly excludes AI systems used "exclusively for military, defence or national security purposes" from its scope. However, this exemption is not absolute; if the same system is used for civilian security, it falls back under the Regulation.

2.1.2. Implementation Scenarios and Opportunities

The following section contrasts implementation strategies under the relevant legal frameworks (GDPR, AI Act, NIS2, NATO Policies) regarding specific technical and procedural aspects.

2.1.2.1. Encryption

Civilian Scenario (EU Law):

[20] Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
[21] NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
[22] Digital Operational Resilience Act: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Requirement: Under DORA (for financial clients) and GDPR[23], EPMwDC must implement "state-of-the-art" encryption for data at rest and in transit. DORA specifically emphasizes the protection of cryptographic keys.

Opportunity: Implementing "end-to-end encryption" for the communication between the EPM sensor and the central reporting server. This is encouraged to safeguard public electronic communications.

Defense Scenario (NATO):

Requirement: NATO's Digital Transformation Strategy calls for a "Digital Backbone" with "security and interoperability engineered by design". Encryption must meet military standards to operate in "denied environments" (e.g., where jamming occurs).

Implementation: The EPM-Mil version should utilize quantum-resistant encryption algorithms, aligning with the "Foster and Protect" strategy for critical technologies.

2.1.2.2. Data Minimization

Civilian Scenario (EU Law):

Requirement: GDPR and the AI Act mandate data minimization. The EPMwDC must not store video feeds indefinitely.

Implementation Strategy (Edge AI): The most viable scenario is Edge AI processing. The camera feed is processed locally on the hardware module; images are discarded immediately, and only metadata (timestamp, location of incident) is transmitted. This aligns with "Privacy by Design".

Defense Scenario (NATO):

Requirement: NATO policies emphasize "Data Exploitation" but balance it with the "need-to-know" principle.

Implementation: While minimization is respected, the system may need to retain raw data (images of the spy) for forensic analysis and "traceability," a core NATO Principle of Responsible Use (PRU)[24].

2.1.2.3. Procedural Aspects

Civilian Scenario (EU Law):

Conformity Assessment: Before placing EPMwDC on the market, the provider must undergo a conformity assessment. If the system is High-Risk, this involves notifying bodies and drawing up an EU declaration of conformity.

Fundamental Rights Impact Assessment (FRIA): Deployers (e.g., a bank using EPM) must verify that the system does not unduly infringe on employee privacy rights before deployment.

Defense Scenario (NATO):

Certification: Instead of a CE mark, the military version would likely require certification through NATO's Data and Artificial Intelligence Review Board (DARB)[25]. The project should create a "DARB-Ready File" or "Responsibility Folder" proving alignment with NATO's 6 PRUs.

Sandboxing: EPMwDC could be tested via DIANA (Defence Innovation Accelerator)[26] to validate performance without triggering civilian regulatory penalties during the R&D phase.

[23] General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[24] NATO AI Strategy (endorsed October 2021; revised July 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

[25] NATO's Data and Artificial Intelligence Review Board (DARB) https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/natos-data-and-artificial-intelligence-review-board

[26] Defence Innovation Accelerator for the North Atlantic (DIANA). https://www.diana.nato.int/

2.1.2.4. Limiting Access to Data

Civilian Scenario (EU Law):

Requirement: DORA requires strict access control policies, limiting physical and logical access to "legitimate and approved functions".

Implementation: Use Role-Based Access Control (RBAC). Only a designated "Security Officer" should be able to view the alert regarding a potential spy; the IT administrator should only see system health logs.

Defense Scenario (NATO):

Requirement: Access is governed by security clearance levels.

Implementation: Integration with the NATO Digital Backbone for interoperability, ensuring that alerts are routed only to command structures with the appropriate clearance.

2.1.2.5. Red Lines, Privacy Impact, and Anonymization

Civilian Scenario (EU Law):

Red Lines: The AI Act prohibits "real-time remote biometric identification" in publicly accessible spaces for law enforcement, with narrow exceptions. If EPMwDC is used in a bank lobby (publicly accessible), identifying who is taking a picture via facial recognition is highly restricted.

Pseudonymization: Personal data must be pseudonymized. If the system detects a leak, it should flag "User ID 12345" rather than "Employee Name," with the re-identification key held separately.

Transparency: Employees must be informed they are subject to the system.

Defense Scenario (NATO):

Red Lines: National security exemptions allow for broader surveillance if the threat is "genuine and present". However, blanket mass surveillance is illegal under CJEU rulings[27].

Balance: The system should focus on object detection (detecting the lens of a spy camera) rather than facial recognition of the operator, to minimize privacy impact while maintaining security efficacy.

2.1.2.6. Division among Civil and Military (Dual-Use) Domains

The "Omni-Use" Trap: Developing a single algorithm for both markets creates legal complexity. If the EPMwDC is marketed as "dual-use," it triggers the Dual-Use Regulation (2021/821)[28] for exports.

The AI Act Boundary: If a system is placed on the market for both civil and military use, it must comply with the AI Act.

Strategic Segmentation: The project should distinguish between EPM-Civ (Civilian) and EPM-Mil (Military) at the design phase.

EPM-Civ: Compliance with AI Act, GDPR, CE marking.

EPM-Mil: Exclusively for defense; exempt from AI Act; subject to national/NATO procurement rules.

2.1.3. Summary of Approaches

The following table summarizes which approaches work better for project implementation, highlighting advantages and pitfalls.

[27] CJEU Case C-413/23 - EDPS v SRB, 2025. https://curia.europa.eu/juris/document/document.jsf?text=&docid=305584&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8121207

[28] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng

Approach	Recommended Strategy	Advantages	Pitfalls
Development Strategy	"Security by Design" (Unified Architecture) Develop a core secure architecture that meets the strictest standard (NATO Reliability + EU Cybersecurity).	Reduces development costs by using one secure baseline. High trust factor for both markets.	Over-engineering for the civilian market may increase costs.
Legal Classification	Strategic Segmentation Clearly separate the product SKU into Civilian and Military versions.	EPM-Mil avoids the bureaucracy of the AI Act. EPM-Civ gains trust via CE compliance.	Risk of "leakage" - if EPM-Mil is used by a police force for civil duties, it inadvertently triggers the AI Act.
Data Handling	Edge Computing (Local Processing) Process video feeds on the device; send only alerts/metadata.	drastic reduction of GDPR liability (Data Minimization). Faster reaction time (Latency).	Less training data collected for model improvement. Difficult to conduct forensic analysis if the local device is destroyed.
Transparency	Explainability by Design The system must explain why it flagged a user (e.g., "lens reflection detected").	Complies with CJEU rulings (Schufa, Dun & Bradstreet) requiring logic explanation. Prevents liability.	revealing the "logic" might allow spies to reverse-engineer the detection method (Trade Secret tension).
Export Control	Dual-Use Licensing Treat the software as a dual-use item under Reg 2021/821.	Ensures legal compliance when selling outside the EU.	Adds administrative burden; requires tracking end-users to prevent human rights violations.

2.1.4. Conclusion for the EU

The most viable implementation scenario for the EPMwDC project is Strategic Segmentation. The developers should build a singular, robust hardware core ("Security by Design") but bifurcate the software and compliance layer.

For the Civilian Market: Focus on privacy preservation via Edge AI. The system should detect the act of espionage (the camera) rather than the actor (the face), thereby lowering the risk classification under the AI Act and GDPR.

For the Military Market: Leverage NATO's DIANA accelerator for testing. Focus on interoperability and "traceability" (forensic data retention) which is permissible under national security exemptions, provided it is targeted and necessary.

2.2. Comparative analysis from the national legal perspective of the Republic of Lithuania

This comparative analysis evaluates the regulatory environment within the Republic of Lithuania for the EPMwDC project. The analysis distinguishes between the Civilian Scenario (e.g., commercial banks, critical infrastructure) and the Defense/Military Scenario (e.g., Ministry of National Defence, Lithuanian Armed Forces), drawing on specific Lithuanian national laws and their intersection with EU and NATO frameworks.

2.2.1. Analysis of the Regulatory Environment of the Republic of Lithuania

Lithuania's regulatory environment is characterised by a strong integration of EU directives (NIS2, GDPR) into national law, alongside distinct, specialised legislation for national security and defence. The country operates a "comprehensive security" model where cyber safety in the civilian sector is closely aligned with national defence interests.

The "Safety Net" (Civilian): The core legal act is the Law on Cybersecurity (Kibernetinio saugumo įstatymas)[29], which transposes the EU NIS2 Directive. It establishes strict cybersecurity risk management and reporting obligations for "essential" and "important" entities (e.g., energy, transport, banking). The State Data Protection Inspectorate (VDAI) oversees GDPR compliance.

Operational Resilience: The National Cyber Incident Management Plan[30] dictates how incidents must be handled and reported. Critical entities must use the National Cybersecurity Centre (NKSC) managed Cybersecurity Information System (KSIS) for registration and reporting.

The Defense/National Security Exemption: Processing personal data for national security or defence is governed by a separate law: the Law on Legal Protection of Personal Data Processed for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or National Security or Defence[31]. This law allows for broader data processing powers but still imposes strict necessity and proportionality requirements.

2.2.2. Implementation Scenarios and Opportunities

The following section contrasts implementation strategies under Lithuanian national law regarding specific technical and procedural aspects.

2.2.2.1. Encryption

Civilian Scenario (Lithuanian Law):

Requirement: The Description of Cybersecurity Requirements (approved by Govt Resolution No 818) mandates that essential and important entities must use encryption for data at rest and in transit. Specifically, sensitive information transmitted via public networks must use encryption (e.g., VPNs).

Implementation: EPMwDC must implement encryption protocols that meet the standards set by the NKSC. Wireless connections must use WPA3 or equivalent strong encryption (EAP/TLS).

Defense Scenario (Lithuanian Defense):

Requirement: Entities on the Secure National Data Transfer Network (Saugusis tinklas) must use specific cryptographic tools approved by the network manager (Ministry of National Defence).

Implementation: If EPMwDC is deployed within the "Saugusis tinklas," it must integrate with the existing secure infrastructure and may require specific, state-approved cryptographic modules rather than standard commercial encryption.

2.2.2.2. Data Minimization

Civilian Scenario (GDPR & National Law):

[29] Law of the Republic of Lithuania on Cybersecurity. https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr

[30] National Cyber Incident Management Plan of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

[31] Law on Legal Protection of Personal Data in Law Enforcement and National Security of the Republic of Lithuania. https://e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/asr

Requirement: The Law on Legal Protection of Personal Data[32] mandates that data collected must be adequate, relevant, and limited to what is necessary. The VDAI guidelines[33] emphasize not collecting more data than needed to solve the specific incident.

Implementation (Edge AI): EPMwDC should process video feeds locally. If a "camera detection" event occurs, the system should ideally only transmit a text alert or a blurred image (pseudonymized) to the central server, deleting the raw video immediately.

Defense Scenario (National Security Law):

Requirement: While data minimization applies, the Law on Personal Data Processed for National Security allows processing "special categories" of data (like biometrics) if strictly necessary for national security.

Implementation: The system may retain raw footage of detected espionage attempts for forensic investigation. However, data must be categorized (factual vs. assessment based) and distinguished between different categories of data subjects (e.g., suspects vs. victims).

2.2.2.3. Procedural Aspects

Civilian Scenario:

Registration: If the client is an "essential" or "important" entity (e.g., a bank), they must register the EPMwDC system details in the Cybersecurity Information System (KSIS) managed by the NKSC.

Incident Reporting: A "significant incident" detected by EPMwDC (e.g., a confirmed spy device affecting critical services) must be reported to the NKSC via the National Cyber Incident Management Plan procedures within strict timelines (early warning within 24 hours).

Defense Scenario:

Accreditation: The system would likely need to undergo a compliance assessment by the National Cybersecurity Centre (NKSC) or military accreditation bodies before being connected to Ministry of National Defence networks.

Exemptions: The AI Act's conformity assessment procedures do not apply if the system is used exclusively for military purposes.

2.2.2.4. Limiting Access to Data

Civilian Scenario:

Requirement: Access control must follow the "least privilege" principle. The Description of Cybersecurity Requirements mandates multi-factor authentication (MFA) and strict password policies for administrators.

Implementation: Access logs must be kept for at least 90 days.

Defense Scenario:

Requirement: Access is strictly governed by the Law on State Secrets and Official Secrets[34] and the specific internal regulations of the "Saugusis tinklas."

Implementation: Integration with the Saugusis tinklas requires compliance with specific organizational and technical requirements set by the network manager. Data flows are restricted and monitored for anomalies.

2.2.2.5. Red Lines, Privacy Impact, and Anonymization

[32] Law of the Republic of Lithuania on the Legal Protection of Personal Data. https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/asr

[33] Methodological information of the State Data Protection Inspectorate. https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/work/

[34] Law on State Secrets and Official Secrets of the Republic of Lithuania. https://www.e-tar.lt/portal/lt/legalAct/TAR.F4CA26A706AF/asr

Civilian Scenario:

Red Lines: Under the Law on Legal Protection of Personal Data, automated decision-making that produces legal effects (e.g., automatically firing an employee detected by EPMwDC) is prohibited without human intervention.

Privacy Impact: A Data Protection Impact Assessment (DPIA) is mandatory before deployment if the system systematically monitors employees. The VDAI has specific guidelines for video surveillance which would likely apply to EPMwDC.

Defense Scenario:

Red Lines: The Law on Personal Data Processed for National Security permits restriction of data subject rights (e.g., right to know they are being monitored) if it would jeopardize a national security investigation.

Balance: Even in defense, the "essence" of fundamental rights must be respected. Mass, indiscriminate surveillance without a specific threat is legally risky under CJEU precedents (e.g., La Quadrature du Net)[35].

2.2.2.6. Division among Civil and Military (Dual-Use) Domains

Civilian Domain: Governed by the Law on Cybersecurity (transposing NIS2) and GDPR. The focus is on resilience and privacy.

Military Domain: Governed by the Law on the Fundamentals of National Security of the Republic of Lithuania[36] and specific exemptions in the Law on Cybersecurity (e.g., intelligence agencies are largely exempt from the standard civilian provisions).

The Dual-Use Challenge: If EPMwDC is marketed to both sectors, the developer must maintain two compliance tracks. The version sold to banks must be CE marked (under the AI Act) and GDPR compliant. The version sold to the military is exempt from the AI Act but must meet NATO/National defense standards.

2.2.3. Summary of Approaches for EPMwDC Implementation

Approach	Recommended Strategy (Lithuania)	Advantages	Pitfalls
Legal Entity Strategy	National Registration Ensure the deploying entity (client) registers the system in the KSIS (Cybersecurity Information System) if they are an "Essential Entity" (e.g., Energy, Transport, Banking).	Ensures compliance with the new Law on Cybersecurity (NIS2). Avoids penalties for non-compliance.	Adds administrative burden. The developer must provide specific technical data for this registration.
Data Handling	Segmentation Treat "Civilian" and "Defense" data flows as completely separate legal environments.	Civilian: Meets strict GDPR/VDAI requirements. Defense: Utilizes the Law on Personal Data Processed for National Security for necessary investigations.	High development cost to maintain separate data governance protocols. Risk of data leakage between environments.

[35] 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

[36] Law on the Fundamentals of National Security of the Republic of Lithuania. https://www.e-tar.lt/portal/it/legalAct/TAR.A0BAB27D768C/asr

Incident Reporting	Automated KSIS Integration Build an API connector to the National Cybersecurity Centre (NKSC) reporting platform.	Enables clients to meet the strict 24-hour / 72-hour reporting deadlines mandated by the National Cyber Incident Management Plan.	Over-reporting of "false positives" could annoy regulators. Thresholds for "Significant Incidents" must be carefully tuned.
Encryption	"Saugusis Tinklas" Compatibility Ensure the system architecture is compatible with the Secure State Data Transfer Network.	Opens the door to government and military contracts (Ministry of Defence, critical state registers).	The "Saugusis tinklas" has strict limitations on internet connectivity, potentially complicating remote updates or cloud features.
Audit & Compliance	Local Certification Engage with the NKSC or accredited auditors for a cybersecurity audit based on the "Description of Cybersecurity Requirements."	Builds trust in the local market. Proves compliance with specific Lithuanian technical mandates (e.g., log retention for 90 days).	Audit cycles are mandatory every 3 years, creating recurring costs.

2.2.4. Conclusion for Lithuania

In Lithuania, the EPMwDC project must navigate a sophisticated regulatory landscape that has recently tightened due to the transposition of the NIS2 Directive into the Law on Cybersecurity.

For the Civilian Market: Success depends on helping clients (banks, energy companies) meet their new "Essential Entity" obligations. The system should automate compliance tasks, such as generating incident reports for the NKSC and maintaining the mandatory 90-day logs.

For the Military/Government Market: The system must be designed to operate within the Secure State Data Transfer Network (Saugusis tinklas). This means it must function effectively with limited or no direct public internet access and support specific state-approved encryption standards. Relying on the specific exemptions in the Law on Personal Data Processed for National Security provides necessary operational leeway for counter-espionage activities that would be illegal in a civilian context.

2.3. Comparative analysis of selected cases outside the scope of the EU legal framework

This comparative analysis evaluates the regulatory environments of the United Kingdom and the United States for the EPMwDC project. Both nations operate independently of EU jurisdiction, though their approaches to AI and data privacy regulation differ significantly - the UK favors a "pro-innovation," sector-led model, while the US is currently characterized by a pivot toward national dominance and federal deregulation, contrasted against a complex patchwork of state-level laws.

2.3.1. Analysis of the Regulatory Environment

United Kingdom (UK)

The UK regulatory framework is defined by a "context-specific" approach rather than a single, overarching AI law. It relies on empowering existing regulators to interpret high-level principles within their specific sectors.

The "Context-Specific" Framework: Instead of a horizontal law like the EU AI Act, the UK uses a framework based on five non-statutory principles: Safety, Security & Robustness; Appropriate Transparency & Explainability; Fairness; Accountability & Governance; and Contestability & Redress.

Key Regulators: Oversight is delegated to sector-specific bodies. For EPMwDC, the key regulators would be the Information Commissioner's Office (ICO)[37] for data privacy, the Competition and Markets Authority (CMA)[38] for market power and foundation model principles, and potentially the Financial Conduct Authority (FCA)[39] if deployed in banking contexts.

Legislative Pillars:

Data (Use and Access) Act 2025[40] (DUAA): Reforms the UK GDPR to simplify data use for scientific research and "recognised legitimate interests" (like national security and crime prevention), introducing a "not materially lower" standard for international transfers.

Digital Markets, Competition and Consumers Act 2024[41] (DMCCA): Focuses on large digital firms with "Strategic Market Status," giving the CMA powers to intervene in digital markets to ensure fair competition.

United States (USA)

The US regulatory environment is currently in a state of flux, characterized by a sharp federal pivot toward deregulation and "AI dominance," conflicting with an aggressive expansion of state-level regulations.

Federal "Dominance" Strategy: The Trump Administration revoked the Biden-era Executive Order 14110 (which emphasized safety guardrails) and issued a new Executive Order, "Removing Barriers to American Leadership in Artificial Intelligence" (Jan 2025)[42]. This new order prioritizes economic competitiveness and directs federal agencies to remove regulatory barriers to AI innovation.

Federal Preemption Efforts: The December 2025 Executive Order, "Ensuring a National Policy Framework for Artificial Intelligence,"[43] established a DOJ task force to challenge state AI laws deemed "onerous" or inconsistent with federal policy, threatening to withhold federal broadband funding from non-compliant states.

The State-Level Patchwork: Despite federal deregulation, strict state laws are taking effect.

California: The Transparency in Frontier AI Act (SB 53)[44] and AI Transparency Act (SB 942)[45] impose strict transparency and safety protocols.

Colorado: The Colorado AI Act (SB 24-205)[46] (effective June 2026) is the first comprehensive US law regulating "high-risk" AI systems, mandating impact assessments for consequential decisions.

Texas: The Responsible AI Governance Act (TRAIGA)[47] regulates AI developers and provides affirmative defenses for following NIST standards.

---

[37] Information Commissioner's Office. https://ico.org.uk/

[38] Competition and Markets Authority. https://www.gov.uk/government/organisations/competition-and-markets-authority

[39] Financial Conduct Authority. https://www.fca.org.uk/

[40] Data (Use and Access) Act 2025. https://www.legislation.gov.uk/ukpga/2025/18/contents

[41] Digital Markets, Competition and Consumers Act 2024. https://www.legislation.gov.uk/ukpga/2024/13/contents

[42] Executive Order 14179 of January 23, 2025. Removing Barriers to American Leadership in Artificial Intelligence. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

[43] Executive Order "Ensuring a National Policy Framework for Artificial Intelligence". https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/

[44] SB-53 Artificial intelligence models: large developers. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53

[45] SB-942 California AI Transparency Act. https://www.leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942

[46] SB24-205 Consumer Protections for Artificial Intelligence. https://leg.colorado.gov/bills/sb24-205

[47] The Texas Responsible AI Governance Act. https://www.nortonrosefulbright.com/en/knowledge/publications/c6c60e0c/the-texas-responsible-ai-governance-act

2.3.2. Implementation Scenarios and Opportunities

2.3.2.1. Encryption

United Kingdom:

Requirement: The Data (Use and Access) Act 2025 maintains UK GDPR standards for security. While specific encryption standards aren't codified in a single "cyber law," the ICO expects robust encryption for personal data.

Opportunity: The Investigatory Powers Act[48] (as amended) includes technical capability notices that can compel operators to remove encryption for national security access. Implementation must balance commercial security with lawful access capabilities if selling to the government.

United States:

Requirement: There is no federal mandate for encryption across the board, but sector-specific laws (e.g., HIPAA for health, GLBA for finance) effectively require it. State data privacy laws (CPRA in California) imply encryption as a "reasonable security procedure."

Opportunity: Adopting the NIST Cybersecurity Framework 2.0 is highly recommended. While voluntary at the federal level, compliance with NIST standards offers an affirmative defense against liability under state laws like the Texas RAIGA and Ohio Data Protection Act.

2.3.2.2. Data Minimization

United Kingdom:

Requirement: The DUAA 2025 retains the UK GDPR's data minimization principle but introduces flexibility. It clarifies that data can be processed for "recognised legitimate interests" (e.g., crime prevention) without a balancing test, potentially allowing EPMwDC to retain more data if justified by security needs.

Scenario: EPMwDC could leverage the "recognised legitimate interest" of crime prevention to justify retaining footage of detected espionage attempts without explicit consent, simplifying compliance compared to the pre-2025 regime.

United States:

Requirement: Data minimization is enforced via a patchwork of state laws. California (CCPA/CPRA) and Colorado (CPA) mandate that data collection be "reasonably necessary and proportionate". The FTC also targets companies for "unfair" data retention practices.

Scenario: Implementation must be state-specific. In Illinois, the Biometric Information Privacy Act (BIPA)[49] requires strict written consent and retention schedules for any biometric data (e.g., face scans of a spy), making "passive" detection legally perilous without explicit opt-ins.

2.3.2.3. Procedural Aspects

United Kingdom:

Approach: Compliance is outcomes-based. The FCA (for fintech clients) or ICO requires assurance that the system is fair and transparent. The CMA focuses on ensuring the AI model doesn't lock clients into a specific ecosystem.

Opportunity: Utilization of the FCA's "AI Live Testing" (sandbox) or the DRCF's AI and Digital Hub allows EPMwDC to test products with regulatory oversight before full market launch, reducing compliance risk.

[48] The Investigatory Powers Act 2016. https://www.legislation.gov.uk/ukpga/2016/25/contents

[49] Biometric Information Privacy Act (BIPA). https://www.aclu-il.org/campaigns-initiatives/biometric-information-privacy-act-bipa/

United States:

Approach: Highly fragmented. Federal guidance (NIST AI RMF) is voluntary but creates a safe harbor. State laws require specific documentation.

Opportunity: California SB 53 requires "frontier developers" (likely not EPMwDC unless it uses a massive model) to publish safety frameworks. However, the Texas RAIGA allows for a regulatory sandbox for AI testing. The most prudent procedural step is to align with the NIST AI RMF, as it satisfies multiple state requirements and aligns with federal procurement standards.

2.3.2.4. Limiting Access to Data

United Kingdom:

Requirement: The DUAA 2025 streamlines data sharing for "public interest" tasks, potentially simplifying access for law enforcement if a spy is detected.

Implementation: Data subject access requests (DSARs) have been modified; organizations can now "stop the clock" while waiting for information to clarify a request, reducing administrative burden.

United States:

Requirement: Access limitations differ by state. California and Colorado provide consumers with rights to access, correct, and delete data.

Implementation: If EPMwDC is used in a workplace, Illinois HB 3773 requires notifying employees if AI is used for monitoring or discipline. Federal preemption efforts are unlikely to remove these consumer/employee access rights in the immediate future.

2.3.2.5. Red Lines and Privacy Impact

United Kingdom:

Red Lines: The UK has resisted a strict "ban" list like the EU's. However, the Online Safety Act imposes duties to prevent harm, particularly if the system could generate illegal content (less relevant for a monitoring tool, but critical if it generates reports/images).

Privacy Impact: A Data Protection Impact Assessment (DPIA) remains standard practice under the ICO guidance.

United States:

Red Lines: Colorado’s AI Act (effective June 2026) imposes a duty of reasonable care to prevent "algorithmic discrimination." If EPMwDC disproportionately flags certain demographics as security threats, it violates this law.

Federal Shift: The FTC has signaled a shift away from banning technologies solely because they could be misused (e.g., setting aside the Rytr order). This suggests a more permissive federal environment for deployment, provided the tool doesn't actively deceive consumers.

2.3.2.6. Division among Civil and Military (Dual-Use) Domains

United Kingdom:

Civil: Governed by the DUAA 2025 and sectoral regulators (FCA, ICO).

Military: The Ministry of Defence (MoD) has its own AI strategy. The National Security and Investment Act allows the government to scrutinize investments in AI companies with dual-use potential.

United States:

Civil: A complex web of state laws and voluntary federal frameworks (NIST).

Military: The "Genesis Mission" Executive Order (Nov 2025)[50] explicitly frames AI as a tool for "global technology dominance" and national security. It directs the Department of Energy to build a shared AI platform for national challenges. EPMwDC could find significant opportunities by positioning itself as a "national security asset" aligned with this new federal directive, avoiding the state-level patchwork by contracting directly with the federal government.

2.3.3. Summary of Approaches

The following table summarizes the strategies for the UK and US markets.

Approach	Recommended Strategy	Advantages	Pitfalls
UK Strategy	"Regulatory Sandbox Engagement" Participate in the FCA's AI Live Testing or DRCF Digital Hub. Align with the Data (Use and Access) Act 2025.	Gaining a "stamp of approval" from UK regulators builds immense trust. The DUAA simplifies lawful grounds for processing security data ("recognised legitimate interests").	The lack of a single AI law means navigating "patchy" guidance across different regulators (ICO, CMA, FCA) creates complexity.
US Strategy	"Federal Alignment & NIST Compliance" Adopt the NIST AI Risk Management Framework (RMF) as the core governance standard.	NIST RMF provides a "safe harbor" affirmative defense in states like Texas. Aligns with federal procurement priorities under the "Genesis Mission".	The conflict between federal preemption efforts and state laws creates legal uncertainty. Relying solely on federal deregulation is risky if state AGs enforce local consumer protection laws.
Data Handling	"Not Materially Lower" (UK) vs. State Specifics (US) UK: Leverage new DUAA flexibility for transfers. US: Use localized data storage or strict segmentation to comply with Illinois BIPA and California CCPA.	UK: Easier data flows to the US under the "Data Bridge". US: Segmentation avoids "poisoning" the whole database with data subject to strict state laws (like Illinois biometric data).	UK: Civil society groups may challenge the UK's data adequacy with the EU due to these looser standards. US: High technical debt to maintain state-by-state compliance logic.
Liability	Conduct-Based (US) vs. Accountability (UK) US: Focus on preventing deceptive use (FTC shift). UK: Focus on Senior Managers & Certification Regime (SM&CR).	US: The FTC is less likely to ban the tool itself, focusing only on misuse. UK: Clear accountability chains satisfy FCA/ICO expectations.	US: State laws (like Colorado's) still impose liability for algorithmic discrimination regardless of federal leniency.

2.3.4. Conclusion from non-EU cases

United Kingdom: The environment is collaborative and sector-led. Success requires deep engagement with specific regulators (ICO, FCA) and utilizing new flexibilities under the Data (Use and Access) Act 2025 to

[50] The "Genesis Mission" Executive Order (Nov 2025). https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/

justify data processing for security purposes. The regulatory sandbox is a unique opportunity to "de-risk" the technology before wider rollout.

United States: The environment is adversarial and bifurcated. The federal government is actively deregulating and pushing for "AI dominance," creating massive opportunities in the defense/federal sector ("Genesis Mission"). However, the civilian market is a minefield of strict state laws (California, Colorado, Illinois). The best path is to adopt the NIST AI RMF to secure safe harbors in state courts while aggressively pursuing federal contracts that may preempt state interference.

3. Content analysis – Recent Policy Practices

3.1. NATO policies and implementation documents – defense domain and dual-purpose domain

NATO recognizes that artificial intelligence (AI) inherently possesses a dual-use nature and addresses it through several key policy and implementation documents designed to govern its use strictly within the defense domain, while promoting collaboration with the civil sector for innovation[51]. These high-level documents establish the principles and strategic direction for AI use in NATO.[52]

NATO's strategic approach is the commitment to Principles of Responsible Use (PRUs) for AI in defense, which are operationalized through a multidisciplinary board to ensure that technological integration remains trustworthy, secure, and aligned with democratic values, human rights, and international law. NATO emphasizes engagement with the European Union (EU) to address the security impacts of EDTs and highlights a "Foster and Protect" strategy focused on dual-use technologies-commercial innovations with critical defense and security applications.

Regarding implementation, NATO underscores security by design through the "secure and trustworthy integration of AI" and data exploitation frameworks. It establishes the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund to harness civilian innovation from start-ups and academia, ensuring that these dual-use tools are developed responsibly before they are fielded. The DARB is specifically tasked with creating a "Responsible AI" certification standard, which serves as a governing mechanism for ethics and accountability in autonomous systems, reflecting a broader effort to maintain a technological edge while mitigating the risks of adversarial exploitation or unintended consequences in both civil and military domains.

3.1.1. NATO Policy Documents

1. NATO AI Strategy (endorsed October 2021; revised July 2024)[53]

Relevance: this is the foundational document for the Alliance's approach to AI. It sets out how NATO aims to accelerate the secure and trustworthy integration of AI for defense and security purposes while safeguarding against threats. It explicitly acknowledges the need to foster development of dual-use technologies that often originate in commercial markets but have defense applications.

The strategy is centered on the Principles of Responsible Use of AI in Defence:

[51] NATO's Strategic Warfare Development Command. Digital Transformation. https://www.act.nato.int/activities/digital-transformation/#:~:text=In%20October%202021%2C%20NATO%20Defence,and%20commitment%20to%20international%20law.

[52] NATO sets a Standard for Ethical Use of New Technologies, News, European Commission. https://ec.europa.eu/newsroom/cipr/items/722501/en#:~:text=The%20upcoming%20adoption%20of%20NATO's,will%20follow%20the%20same%20approach.

[53] NATO AI Strategy (endorsed October 2021; revised July 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

- Lawfulness
- Responsibility and Accountability
- Explainability and Traceability
- Reliability
- Governability
- Bias Mitigation

Strategy (July 2024) emphasizes the accelerated adoption of secure and trustworthy AI while strictly adhering to NATO's six Principles of Responsible Use (PRUs): Lawfulness, Responsibility and Accountability, Explainability and Traceability, Reliability, Governability, and Bias Mitigation. The strategy identifies quality data as a fundamental prerequisite, noting that AI-ready data must be trusted and free from unintended bias to ensure the development of reliable systems. It explicitly addresses the dual-use nature of AI, focusing on the challenges of integrating civilian-market solutions into defense and the need to mitigate risks from adversarial use, such as AI-enabled disinformation and information operations that threaten democratic trust.

It also reflects concerns through its commitment to "Responsible AI" certification standards, assessment templates, and a 360-degree monitoring of technology trends. It highlights increased cooperation with the European Union (EU) as a key objective to facilitate information exchange and the sharing of best practices in AI safety and accreditation. Furthermore, the strategy promotes "Security by Design" principles by calling for the establishment of an Alliance-wide Testing, Evaluation, Verification, and Validation (TEV&V) landscape and utilizing specialized "sandboxes" to ensure that AI applications are safe and compliant with international law before deployment.

2. NATO 2022 Strategic Concept[54]

Relevance: this document outlines the Alliance's overall purpose and approach to security challenges, emphasizing the need to enhance NATO's technological edge (including AI) to strengthen deterrence and defense across all domains (land, air, maritime, cyber, and space).

The NATO 2022 Strategic Concept defines the European Union (EU) as a unique and essential partner, emphasizing the need for enhanced cooperation on issues of common interest, including emerging and disruptive technologies, resilience, and countering cyber and hybrid threats. The Alliance underscores the cross-cutting importance of investing in technological innovation and explicitly commits to adopting and integrating new technologies by cooperating with the private sector and shaping standards based on principles of responsible use that reflect democratic values and human rights. NATO specifically identifies cyberspace as a contested domain where malign actors target critical infrastructure and government services, leading to a commitment to expedite digital transformation and enhance cyber defenses as a collective responsibility.

The document also addresses the security implications of dual-use technologies, noting that strategic competitors such as the Russian Federation are expanding novel and disruptive dual-capable delivery systems. To retain its technological edge, NATO aims to protect its innovation ecosystems and work with international organizations like the EU to tackle the conditions conducive to the spread of terrorism and other shared security challenges. While the text does not explicitly name the "EU Artificial Intelligence Act" or "GDPR," it establishes a strategic vision for promoting responsible behavior in cyberspace and space, recognizing the applicability of international law to these domains.

3. "Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies (EDTs)" (February 2021)[55]

[54] NATO 2022 Strategic Concept. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

[55] "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

Relevance: this overarching strategy guides NATO's relationship with EDTs, focusing on both fostering the development of dual-use technologies and creating a framework to protect those technologies from being used against the Alliance.

NATO's policy on Emerging and Disruptive Technologies (EDTs) focuses on fostering and protecting nine priority areas-including artificial intelligence (AI), quantum technologies, and next-generation communications-through a strategy that prioritizes dual-use applications developed by commercial markets but applicable to defense. A central provision is the 2021 Artificial Intelligence (AI) Strategy, which established the Principles of Responsible Use (PRUs) and created the Data and AI Review Board (DARB) to operationalize these principles through a "Responsible AI" certification standard and practical toolkits for Allies. The document underscores the critical role of data as an enabler, governed by the Data Exploitation Framework Policy, which aims to mainstream the secure and trustworthy integration of technology while protecting against adversarial threats and ensuring adherence to international law.

It should be highlighted NATO's active engagement with the European Union (EU) and other international organizations to address shared security challenges posed by EDTs. The strategy reflects a commitment to "Security by Design" principles through initiatives like the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund, which engage with academia and the private sector to develop secure, resilient, and ethically grounded technologies. These efforts are designed to ensure that AI and other critical technologies are integrated into Alliance capabilities in a manner that reflects democratic values, human rights, and the rule of law.

4. Data Strategy for the Alliance (May 2025)[56]

Relevance: this provides a framework for guiding NATO's transition to becoming a data-centric organization, which is a prerequisite for effective AI implementation. It emphasizes modern standards for data interoperability to ensure seamless collaboration between humans and technology.

The Data Strategy for the Alliance (May 2025) outlines NATO's transition into a data-centric organization, emphasizing the use of computational data governance to maintain data quality, security, and privacy at scale. It establishes a cohesive framework for managing data as a strategic asset, balancing the "responsibility to share" with "need-to-know" principles while ensuring compliance with security, legal, and privacy obligations. The strategy specifically highlights Security by Design and Privacy by Design through the implementation of a "Data Centric Reference Architecture" (DCRA) and the use of modern standards like STANAG 5636 to ensure semantic interoperability, which is vital for the effective and ethical use of Artificial Intelligence (AI) across the Alliance.

The document refers to the necessity of adhering to international agreements and approved NATO policies regarding data protection and legal restrictions. The strategy promotes the creation of shared data spaces and federated meshes to enable controlled data sharing, which directly supports AI security and helps mitigate risks associated with dual-use technologies by fostering trusted partnerships with industry and academia. Furthermore, it designates the Digital Policy Committee and the NATO Chief Information Officer (OCIO) as central bodies for overseeing policy implementation and ensuring that data management practices reflect the Alliance's core values of transparency and accountability.

3.1.2. Implementation Documents and Mechanisms

These documents and bodies translate the high-level policies into practical actions, particularly concerning the dual-use domain:

1. NATO's Data and Artificial Intelligence Review Board (DARB)[57]

[56] 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

[57] NATO's Data and Artificial Intelligence Review Board (DARB) https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/natos-data-and-artificial-intelligence-review-board

Relevance: established in October 2022, the DARB is the central governance body responsible for operationalizing the Principles of Responsible Use of AI. It is developing a "Responsible AI" certification standard and practical toolkits to guide AI implementation.

The Establishment of NATO's Data and Artificial Intelligence Review Board (DARB) (October 2022) outlines the board's mission to operationalize NATO's six Principles of Responsible Use (PRUs): lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation. The DARB's primary function is to translate these ethical principles into user-friendly Responsible AI (RAI) standards and a certification process for the NATO Enterprise, aimed at mitigating risks and ensuring the adoption of trustworthy, interoperable AI systems. It emphasizes a "responsible-by-design" approach, directing Allies to implement quality controls that align with international law and democratic norms.

Furthermore, the board serves as a multidisciplinary forum-comprising experts from government, academia, and the private sector-to share best practices and exchange views on AI governance. Its key deliverable, the RAI certification standard, draws from best practices in both the defense sector and civilian-oriented initiatives, addressing the dual-use nature of AI by fostering engagement with academic and civil society actors. This certification process is intended to ensure that AI applications are safe and reliable, providing a qualitative advantage over strategic competitors while maintaining public trust and adherence to legal and ethical requirements in both civil and defense domains.

2. Autonomy Implementation Plan (October 2022)[58]

Relevance: this plan drives a coherent approach to the development and protection of autonomous systems, ensuring they align with the Alliance's values and international law.

NATO's Autonomy Implementation Plan (October 2022) emphasizes that the responsible development and use of autonomous systems must be anchored in NATO's norms, values, and international law, specifically applying the six Principles of Responsible Use (PRUs) for AI-lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation. The plan focuses on building trust in these technologies through "responsible-by-design" practices and ensures that AI-enabled autonomous systems are subject to operational trust and public accountability. It highlights the critical role of data and AI as enablers for autonomy and the need to protect these systems from adversarial interference, deception, and the unauthorized acquisition of sensitive technologies.

Regarding lethal autonomous weapons systems (LAWS), NATO aligns with the 2019 guiding principles of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW), reaffirming that international humanitarian law applies fully to all weapons systems. The implementation plan also addresses the dual-use nature of these technologies, recognizing that strategic competitors are investing heavily in autonomous systems to achieve asymmetric advantages. Consequently, NATO aims to establish clear pathways for integrating these systems into military operations while fostering public trust and countering disinformation that could erode societal confidence in the military use of autonomy.

3. NATO's Digital Transformation Implementation Strategy (October 2024)[59]

Relevance: a roadmap to leverage digital technology, including AI, for multi-domain operations and data-driven decision-making, ensuring interoperability across different domains.

The NATO's Digital Transformation Implementation Strategy (October 2024) outlines a comprehensive plan to modernize the Alliance for the information age, emphasizing the shift toward a data-centric architecture and the establishment of a "Digital Backbone" to enable seamless collaboration across all operational domains. A key provision is the commitment to "security and interoperability engineered by design," which requires modern standards and coherent governance to ensure that capabilities remain resilient and future-proof. The strategy explicitly integrates cybersecurity and cyber defense into its relevant

[58] Autonomy Implementation Plan (October 2022). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/summary-of-natos-autonomy-implementation-plan

[59] NATO's Digital Transformation Implementation Strategy (October 2024). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/17/natos-digital-transformation-implementation-strategy

lines of effort, connecting them to NATO and Allied initiatives to bolster the protection of trusted data and infrastructure. It underscores the shared responsibility of Allies to address data management and protection requirements, particularly within the newly established Alliance Data Sharing Ecosystem.

Furthermore, the strategy highlights the importance of data-centric governance and the exploitation of advanced analytics and AI capabilities to enhance situational awareness and data-driven decision-making. It calls for the creation of an environment where data from Allies, the NATO Enterprise, and industry partners is securely shared and connected, while strictly respecting NATO's Principles of Responsible Use of AI and Data. By fostering a digital-ready workforce and broadening cooperation with academia and the private sector, NATO aims to mitigate risks associated with dual-use technologies and adversarial exploitation. This approach is intended to ensure that the Alliance can maintain its technological edge while adhering to fundamental values of transparency, accountability, and legal compliance in both civil and defense contexts.

4. Defence Innovation Accelerator for the North Atlantic (DIANA)[60]

Relevance: DIANA connects military operational needs with the dual-use technological expertise of start-ups, academia, and industry. Its core mission is to promote innovation in dual-use emerging and disruptive technologies, including AI, to solve critical defense and security challenges.

The Defence Innovation Accelerator for the North Atlantic (DIANA) identifies the organization as a NATO body established to find and accelerate dual-use innovation capacity by engaging with researchers and entrepreneurs to solve critical defense and security challenges. DIANA's primary mechanism for implementation is through industry challenges that require innovators to develop deep-tech solutions for collective resilience and operation in denied environments. DIANA's role can be highlighted in providing testing, demonstration, and validation across approximately 180 test centres to de-risk technological solutions before they enter the market.

Regarding security and ethics, the initiative reflects a commitment to supporting a "peaceful future" by guiding innovators through a network of mentors, including government procurement experts and scientists, to ensure technologies meet Alliance needs. This ecosystem is designed to bridge the gap between civilian innovation and defense requirements, ensuring that dual-use tools are robust and reliable. Furthermore, the platform facilitates pathways to both the NATO enterprise and 32 Allied markets, which necessitates that participating companies align their innovations with the broader NATO and EU regulatory landscapes governing cybersecurity and data protection.

5. NATO Innovation Fund[61]

Relevance: a venture capital fund that invests in start-ups developing dual-use technologies in priority areas like AI, further bridging the civil-military gap.

The NATO Innovation Fund (NIF) is the world's first multi-sovereign venture capital fund, deploying over €1 billion in deep tech to secure the future of the Alliance's 1 billion citizens. Backed by 24 NATO Allies, including Lithuania, the fund acts as a "strategic impact" and "patient capital" vehicle, investing directly and indirectly in startups developing Emerging and Disruptive Technologies (EDTs)-such as Artificial Intelligence (AI), Autonomy, and Next-Generation Communications-that have critical dual-use applications for both civilian and defense sectors.

Alignment with Cybersecurity, Data Protection, and Ethics. The NIF explicitly integrates NATO's Principles of Responsible Use (PRUs) into its investment process and ongoing monitoring to ensure that technological advancements align with democratic values, international law, and human rights. Its Responsible Investment Policy emphasizes:

- Safety and Security by Design: NIF analyzes investee companies' operational processes, focusing on governance, legal/regulatory compliance, and data privacy and security.

[60] Defence Innovation Accelerator for the North Atlantic (DIANA). https://www.diana.nato.int/
[61] The NATO Innovation Fund. https://www.nif.fund/

- Accountability in AI: Guided by the PRUs, the fund requires transparency, explainability, and bias mitigation in AI systems, ensuring they are subject to proper human oversight and "governability" (e.g., the ability to deactivate a system).
- Compliance with EU/International Standards: While the NIF operates independently, its mission to build a vibrant defense ecosystem involves close collaboration with the European Investment Fund (EIF) and the European Commission. This partnership aims to unlock private capital while ensuring that startups meet ethical and legal criteria, such as those set out in the EU SFDR (Sustainable Finance Disclosure Regulation) and the GDPR.

Strategic Partnerships and Dual-Use Focus.The NIF serves as a bridge between the commercial and government markets, helping deep-tech founders navigate the "Valley of Death" through long-term (15-year) capital. Key initiatives include:

- EIF-NIF Partnership (July 2024): A Memorandum of Understanding (MoU) was signed to expand funding for startups and SMEs in the defense and resilience sectors, fostering a comprehensive investment ecosystem that supports technological sovereignty for both NATO and the EU.
- Operational Validation: The fund works with NATO initiatives like Task Force X to test uncrewed and autonomous technologies in real operational environments, building trust through practical demonstration and rapid feedback loops with military users.
- Exclusion Policy: The NIF maintains strict ethical boundaries, refusing to invest in companies involved in the production or trade of weapons prohibited by international law, such as anti-personnel mines or cluster munitions.

3.2. EU policy and implementation documents – civil domain and dual-purpose domain

The EU AI Act takes a nuanced but firm position on dual-use AI systems: they are subject to the Act's regulations whenever they have a civilian application within the EU market[62], even if they also possess military potential.

Experts emphasize that while the EU AI Act establishes a comprehensive risk-based framework to protect fundamental rights, it explicitly excludes AI systems developed or used solely for national security, defense, and military purposes. This exclusion is based on the principle that national security remains the sole responsibility of individual EU Member States. However, the Act does apply to dual-use technologies if they are also deployed for civilian, humanitarian, or law enforcement purposes. This is particularly relevant for the national security community, as many defense-related AI capabilities are procured or adapted from private industry rather than developed from scratch. Furthermore, the Act encompasses law enforcement, requiring a careful review of shared capabilities between national security and police services to ensure compliance with prohibitions on systems like predictive policing and real-time biometric identification.

Regarding implementation, it has to be emphasized that national security agencies can voluntarily adopt the Act's best practices for risk management, including its stringent requirements for cybersecurity, robustness, and accuracy outlined in Article 15. The Act is also expected to accelerate the development of international technical standards and increase industry-provided documentation for high-risk and general-purpose AI, which will likely facilitate AI assurance and procurement for national security customers. By mandating transparency and adversarial testing for systemic-risk models, the EU AI Act indirectly strengthens the "security by design" baseline for dual-use technologies, helping national security organizations navigate complex AI lifecycles while maintaining necessary scrutiny to avoid unintended consequences.

Moreover, while the Regulation covers dual-use systems-those intended for both civilian and military applications-it leaves purely military AI to the individual responsibility of Member States under the Treaty on European Union. This omission is identified as a significant concern given AI's "immense transformative

[62] R. Powel. The EU AI Act: National Security Implications. Centre for Emerging Technology and Security (August 2024). https://cetas.turing.ac.uk/sites/default/files/2024-07/cetas_explainer_-_the_eu_ai_act_-_national_security_implications.pdf

capacity" in areas such as defense innovation, surveillance, logistical operations, and cybersecurity. Some experts argue that without a unified EU framework for military AI, the region remains vulnerable to non-conventional threats, including AI-enabled information operations and disinformation that could sow division and erode democratic trust.

To address these implementation gaps, might be recommended that the revised EU AI Act incorporates dedicated chapters on military AI to establish shared standards for forecasting and early warning procedures. It should underscore the need for "Security by Design" and AI ethics to prevent the escalation of conflicts caused by over-reliance on biased or improperly tested machine-generated outputs. Furthermore, it should be stressed the importance of protecting sensitive patient and geopolitical data from cyberattacks when AI systems interact across different platforms. Establishing common rules for military AI cooperation would not only strengthen the EU's common security and defense policy but also ensure that decision-making processes-particularly in high-stakes foreign policy-are anchored in responsible AI principles that protect human rights and international law[63].

3.2.1. Key Principles for Dual-Use AI under the EU AI Act

- Exclusion for Purely Military Use: The only explicit exemption in the EU AI Act (Article 2) is for AI systems developed and used exclusively for military, defense, or national security purposes by relevant public authorities[64].
- Civilian Use Triggers Compliance: If a system has a dual function and is placed on the EU market, or its output impacts people in the EU, for any civilian purpose (e.g., law enforcement, public safety, healthcare, transport), the Act applies to that civilian application[65].
- "Omni-use" Technology: Many modern technologies, including advanced AI, are increasingly considered "omni-use" due to their simultaneous application across various domains (defense, health, industry, etc.). The Act recognizes this reality by ensuring that non-military uses are still regulated to protect fundamental rights and safety.
- General-Purpose AI (GPAI) and Systemic Risk: The Act introduces specific rules for GPAI models, which many experts inherently view as dual-use due to their broad potential for both beneficial and malicious applications (e.g., in cyberattacks or biological weapon development).
    - Providers of all GPAI models have transparency and documentation obligations.
    - GPAI models with "systemic risk" (based on high-impact capabilities or significant compute used for training) face stricter obligations, including risk assessments, incident reporting, and model evaluations.

Speaking more broadly about the above principles, the Centre for Future Generations (CFG) report, "Double-edged tech: Advanced AI & compute as dual-use technologies" (2025)[66], analyzes the global governance of advanced AI, noting that while the EU AI Act does not explicitly use the term "dual-use," it effectively addresses dual-use risk factors such as public deception and general risks to citizens' health and

[63] S. Kulueva, A. Grigoriescu (ed.). Blind Spots in AI Governance: Military AI and the EU's Regulatory Oversight Gap. ES Think Tank (October 2025). https://esthinktank.com/2025/10/03/blind-spots-in-ai-governance-military-ai-and-the-eus-regulatory-oversight-gap/#:~:text=Accordingly%2C%20while%20the%20Regulation%20excludes,responsibility%20of%20each%20member%20state.

[64] Review of the EU Artificial Intelligence Act. https://artificialintelligenceact.eu/article/2/#:~:text=Summary,or%20fall%20under%20certain%20articles.

[65] European Commission Press corner - Questions and answers regarding Artificial intelligence (August 2024). https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683

[66] Centre for Future Generations. "Double-edged tech: Advanced AI & compute as dual-use technologies" (2025). https://cfg.eu/double-edged-tech/#:~:text=The%20US%20Executive%20Order%20on%20the%20Safe%2C%20Secure%2C%20and%20Trustworthy,cases%20such%20as%20weapon%20generation

safety. The report highlights that advanced AI models currently lack a robust, multilateral governance framework to mitigate risks like automated cyber-attacks or the optimization of weapon systems. It identifies a critical implementation challenge: current AI evaluations are often limited to pre-deployment stages and lack internationally accepted standards, necessitating more rigorous security by design measures that are not yet globally enforced.

Regarding data and cybersecurity, the document emphasizes that dual-use risks are directly linked to the capabilities of AI models and the physical compute resources required to train them. It suggests that regulating compute resources could offer an alternative framework for managing the dual-use nature of AI, as the software itself is inherently difficult to govern. While the report does not detail specific GDPR or Privacy by Design provisions, it underscores the need for an end-to-end governance framework involving model capability assessors and a coordinating body to report findings on potential security breaches. This approach aims to prevent the misuse of dual-use items by hostile actors while still allowing for legitimate civilian applications in line with international agreements like the Wassenaar Arrangement.

The recent article from "Leupold Legal"[67] emphasizes that the EU AI Act explicitly excludes AI systems used solely for national security, defense, and military purposes under Article 2(3), as these areas fall within the exclusive competence of individual Member States. However, the article highlights a critical functional distinction for dual-use AI: if a system developed for defense is temporarily or permanently used for civilian, humanitarian, or public security purposes, it must comply with the AI Act's requirements. Conversely, military use of a civilian-market AI system-such as for territorial integrity or ISR (intelligence, surveillance, and reconnaissance)-remains exempt from the regulation. This functional approach ensures that while the EU ensures AI security and ethics in the civilian sphere, it does not directly impede the primary tasks of the armed forces, which are already subject to the laws of armed conflict and national regulations.

Regarding implementation, the article emphasizes that providers of dual-use systems must ensure compliance for non-military use cases to address risks to public safety and order. It notes that the EU's lack of legislative competence to regulate purely military AI is anchored in Article 4(2) of the Treaty on European Union, as reaffirmed by the European Court of Justice (ECJ). While the document does not explicitly name GDPR or specific "Privacy by Design" engineering principles, it argues for a proactive development strategy where civilian AI systems are designed with the flexibility to be adapted for defense at a reasonable economic cost. This "Security by Design" approach aims to promote military innovation while maintaining a clear division of competences between the Union's civilian safety standards and the Member States' national security requirements.

3.2.2. Practical Implications for Businesses and Developers

- Design Consideration: Companies developing AI systems with potential dual-use applications (e.g., drones, advanced materials software, certain sensors) should consider the AI Act's compliance requirements from the design phase, particularly if civilian market access is desired[68].
- Segmentation of Use Cases: It may be necessary to clearly delineate the military vs. civilian use cases and ensure that the civilian variants meet all relevant AI Act requirements, which may involve separate documentation and conformity assessments.
- Interplay with Export Controls: The AI Act operates alongside existing EU dual-use export control regulations (Regulation (EU) 2021/821). A dual-use classification under the AI Act might also trigger the need for specific export licenses when exporting outside the EU, adding layers of compliance.

[67] The Leupold Legal. "Does the EU AI Act jeopardize Europe's defense readiness?" (November 2025). https://leupoldlegal.com/does-the-eu-ai-regulation-jeopardize-europes-defense-readiness/#:~:text=Although%20it%20has%20been%20pointed,it%20already%20complies%20with%20it

[68] Gregory Smith, Karlyn D. Stanley, Krystyna Marcinek, Paul Cormarie, Salil Gunashekar.General-Purpose Artificial Intelligence (GPAI) Models and GPAI Models with Systemic Risk: Classification and Requirements for Providers (August 2024). https://www.rand.org/pubs/research_reports/RRA3243-1.html

- Downstream Provider Obligations: Providers of GPAI models must cooperate with downstream providers to help them comply with their own obligations when integrating the model into a high-risk AI system.

In essence, the EU AI Act ensures a comprehensive safety net for AI use within the Union by making the intended application the decisive factor in its scope, rather than allowing a military potential to exempt all development of a technology.

The European Policy Centre (EPC) report, "From Dual-Use to Omni-Use: Securing Europe's Future" (2025), argues that traditional "dual-use" classifications are obsolete in an era where technologies like Artificial Intelligence (AI), additive manufacturing, and quantum sensing operate simultaneously across defense, health, and industrial domains-a concept termed "omni-use." The report emphasizes that rigid binary logic in current laws, such as the EU Dual-Use Regulation, slows innovation and imposes unnecessary compliance burdens on the private sector. To address this, it recommends a shift toward "omni-use by design" in research and innovation frameworks (e.g., Horizon Europe and the European Defence Fund), requiring developers to anticipate cross-sectoral applications from the outset to ensure resilience and competitiveness.

Regarding implementation, the report highlights the Cyber Resilience Act as a critical step in imposing cybersecurity obligations across all digital products, recognizing that vulnerabilities in consumer devices can cascade into defense supply chains. It underscores the need for updated governance structures, such as regulatory sandboxes, where startups can test omni-use applications without being paralyzed by fragmented regulatory requirements. While it does not explicitly detail "GDPR" provisions, the report reflects a broader commitment to security and privacy by design by calling for standing coordination mechanisms between defense ministries and civil regulators to manage the ethical and security dilemmas inherent in technologies that underpin both societal resilience and military readiness[69].

3.2.3. Key EU Policy Documents (Excluding Regulations & Directives)

It has to be noted that the EU AI Act is a Regulation, but its interpretation and application to dual-purpose (civil-military) domains are shaped by a broader ecosystem of policy documents and foundational case law.

Because the AI Act is new (fully applicable as of mid-2026, with some provisions earlier), there are no ECJ judgments directly interpreting it yet. However, the Court has established critical legal principles on automated decision-making and national security exemptions that will define how the Act is applied.These "soft law" and strategic documents provide the rationale for how the EU manages the overlap between civilian AI safety and defence/security needs.

A. Specific to Dual-Use, Defence & Security

1. Action Plan on Synergies between Civil, Defence and Space Industries (Feb 2021)[70]

Relevance: This is the primary policy blueprint for "cross-fertilization." It explicitly aims to break down the walls between civil and defence research, encouraging the use of "dual-use" technologies like AI for both commercial and military applications to boost EU innovation.

Action Plan on Synergies between Civil, Defence and Space Industries, outlines a strategic framework to enhance "cross-fertilization" between these sectors, with a specific focus on maintaining the EU's technological sovereignty and leadership in digital technologies. While the document predates the final EU

[69] European Policy centre. From Dual-Use to Omni-Use: Securing Europe's Future (October 2025). https://www.epc.eu/publication/from-dual-use-to-omni-use-securing-europes-future/

[70] 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

AI Act, it identifies Artificial Intelligence (AI), cybersecurity, and data cloud infrastructures as "critical technologies" where synergies between civil and defense domains offer substantial potential. A central provision is the promotion of a Capability Driven Approach (CDA) for the security sector, which is intended to facilitate the use of innovative technologies by law enforcement while ensuring mandatory compliance with European data protection (GDPR) and ethical standards.

Regarding implementation, the Action Plan emphasizes Security by Design and Privacy by Design principles through the development of hybrid civil/defense standards and the establishment of an EU Observatory of Critical Technologies to monitor dependencies and gaps. It highlights the creation of a Cybersecurity Competence Centre (CCC) and the launch of flagship projects, such as a space-based global secure communications system integrating quantum encryption, to protect critical infrastructure from large-scale cyber-attacks. The document also explicitly recognizes the importance of EU-NATO cooperation as a relevant factor for interoperability and seeks to bridge the fragmented civil-defense innovation landscape by establishing an "innovation incubator" and supporting cross-border defense innovation networks to ensure the responsible and secure deployment of dual-use technologies.

2. Roadmap on Critical Technologies for Security and Defence (Feb 2022)[71]

Relevance: Identifies AI as a "critical technology" where the EU must reduce strategic dependencies. It calls for a more coordinated approach to research that serves both security and civilian needs, directly reinforcing the "dual-purpose" reality.

The Commission Communication COM(2022) 61, "Roadmap on critical technologies for security and defence," outlines a strategic framework for the EU to achieve technological sovereignty by reducing dependencies on third countries for critical technologies, including Artificial Intelligence (AI), semiconductors, and cybersecurity. The document emphasizes the need for a "balanced approach" to dual-use innovation, acknowledging that the civilian sector increasingly drives breakthroughs that are vital for defense. While it predates the final enactment of the EU AI Act, the Roadmap explicitly identifies AI as a priority area where the EU must establish its own standards to ensure AI security and ethics, preventing the adoption of non-EU standards that might conflict with European values and fundamental rights.

Regarding implementation, the Roadmap promotes "security by design" by proposing the establishment of an EU Observatory of Critical Technologies to monitor value chains and identify strategic vulnerabilities. It highlights the importance of EU-NATO cooperation as a key pillar for ensuring interoperability and a common transatlantic approach to protecting critical infrastructures from cyber threats. Although the document does not detail specific GDPR or Privacy by Design provisions, it underscores that all technological developments in the security and defense sectors must adhere to established EU priorities, including the high standards of data protection and the rule of law. The roadmap further advocates for the use of regulatory sandboxes to test dual-use innovations, ensuring they are safe and ethically grounded before being scaled for military or civil-protection purposes.

3. White Paper on Export Controls (Jan 2024)[72]

Relevance: Addresses the risk of dual-use technologies (including advanced AI) being used by foreign adversaries. It proposes mechanisms to better control the export of such technologies without stifling innovation, complementing the AI Act's safety focus with security controls.

The European Commission White Paper on options to enhance support for research and development involving technologies with dual-use potential (COM(2024) 25) addresses the critical need to bridge the historical gap between exclusively civil and exclusively defense R&D. While the document does not explicitly cite the "EU AI Act" or "GDPR," it defines dual-use consistent with Regulation (EU) 2021/821, focusing on software and technologies-such as Artificial Intelligence (AI) and cybersecurity tools-that serve

[71] Roadmap on critical technologies for security and defence COM(2022) 61 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0061

[72] White Paper on Export Controls COM(2024) 25 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025

both civilian and military strategic objectives. A central provision is the proposal to remove the "exclusive focus on civil applications" in parts of the successor to Horizon Europe (Framework Programme 10), thereby encouraging synergies that allow civilian-driven innovations to strengthen the defense industrial base and accelerate the deployment of high-stakes services.

Regarding implementation, the White Paper explores creating a more integrated framework for dual-use R&I to reduce strategic dependencies and enhance technological sovereignty within the EU and across the transatlantic partnership with NATO. It emphasizes a "dual-use by design" approach, which encourages developers to anticipate cross-sectoral applications from the initial stages of research, particularly for emerging technologies like quantum and aerospace. The document highlights that such integration must balance innovation with ethical assessments to prevent military misuse, aligning with broader EU values of transparency and fundamental rights while ensuring that R&D activities under instruments like the European Innovation Council (EIC) effectively support both commercial competitiveness and regional security.

4. EU Strategic Compass for Security and Defence (March 2022)[73]

Relevance: A high-level political strategy that sets out the EU's ambition to become a stronger security provider, explicitly mentioning the need to invest in and secure emerging technologies like AI for defence purposes.

The EU Strategic Compass for Security and Defence identifies the European Union (EU) and NATO as sharing a strategic environment where emerging and disruptive technologies, particularly Artificial Intelligence (AI) and cyber capabilities, are central to global competition. The document underscores the growing importance of defense innovation and emphasizes the need to strengthen emerging military technologies, including AI, to ensure operational resilience and strategic autonomy. While it does not explicitly cite the "GDPR" or "Privacy by Design" technical standards, it stresses that the EU's approach to AI must be human-centric and risk-based, explicitly excluding purely military use from the EU AI Act while acknowledging that dual-use applications remain subject to civilian ethical and legal standards.

Regarding implementation, the Strategic Compass highlights the need for robust cybersecurity measures and global cooperation in military AI regulation to prevent conflict escalation due to reduced human oversight. It calls for the integration of ethical guidelines into defense AI and supports international efforts to regulate lethal autonomous weapons (LAWS), affirming the principle of "meaningful human control". Furthermore, the document promotes synergies between the civilian and defense industries through initiatives like the European Defence Fund, ensuring that technological advancements in the cyber and AI domains adhere to international humanitarian law and contribute to the collective security of both the EU and its NATO allies.

5. Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council - "Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence (2025)[74]

Relevance: Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council - "Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence focuses on strengthening cybersecurity through the implementation of the Cyber Resilience Act and the Cyber Solidarity Act, aiming to improve detection, preparedness, and response to large-scale threats, alongside the Network and Information Security (NIS) Directive for critical infrastructure.

Regarding EU-NATO cooperation, the text highlights the launch of new Structured Dialogues specifically covering cyber issues and emerging and disruptive technologies. In the domain of dual-use and AI, the report notes the adaptation of European Investment Bank (EIB) lending definitions to support dual-

[73] EU Strategic Compass for Security and Defence. https://www.consilium.europa.eu/en/policies/strategic-compass/
[74] Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council - "Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence (2025). https://data.consilium.europa.eu/doc/document/ST-8023-2025-INIT/en/pdf

use goods for the security and defence industry, conducts risk assessments on AI technology leakage, and mentions the integration of artificial intelligence in war gaming concepts.

6. European Defence Industrial Strategy (EDIS) (March 2024)[75]

Relevance: Promotes the integration of civilian innovation (often AI-driven) into the defence sector, further blurring the lines the AI Act seeks to regulate.

The European Defence Industrial Strategy (EDIS) Joint Communication (March 2024) outlines a comprehensive plan to increase the EU's defense readiness through a more resilient and innovative European Defence Technological and Industrial Base (EDTIB). The strategy explicitly identifies Artificial Intelligence (AI), cybersecurity, and space domain awareness as critical "strategic enablers" and "disruptive technologies" where the Union must achieve technological supremacy to counter hybrid threats, including cyberattacks, disinformation, and hacking of critical infrastructure. While the document does not name the "EU AI Act" or "GDPR" explicitly, it emphasizes the necessity of a "Security by Design" approach-proposing a network of cyber defensive capabilities and the launch of "European Defence Projects of Common Interest" to secure access to contested areas like the cyber and space domains.

Regarding the dual-use nature of these technologies, EDIS highlights the increasing role of civilian innovation (e.g., in drones and semiconductors) in driving defense capabilities, advocating for a "Capability Driven Approach" to better integrate civilian breakthroughs while ensuring interoperability with NATO. The strategy proposes the creation of a European Defence Industry Group and an "Innovation Office" in Kyiv to bridge the gap between startups and military needs, thereby fostering a "trust dividend" for EU-made solutions. Furthermore, it calls for the development of hybrid civil/defense standards-building on NATO STANAGs-to enhance operational effectiveness and ensure that technological advancements in the cyber and AI realms are robust, scalable, and compliant with broader European security priorities.

7. WHITE PAPER On options for enhancing support for research and development involving technologies with dual-use potential.[76]

Relevance: The European Commission White Paper on options to enhance support for research and development involving technologies with dual-use potential (COM(2024) 25) addresses the historical separation between civilian and defense R&D, proposing options to bridge this gap particularly for critical technologies like Artificial Intelligence (AI) and cybersecurity tools. While the document does not explicitly cite the "EU AI Act" or "GDPR," it defines dual-use consistent with Regulation (EU) 2021/821, focusing on software and technologies that serve both civilian and military strategic objectives. A central provision is the potential removal of the "exclusive focus on civil applications" in parts of the successor to Horizon Europe (Framework Programme 10), which would encourage synergies that allow civilian-driven innovations to strengthen the defense industrial base and accelerate the market uptake of high-stakes services.

Regarding implementation, the White Paper explores creating a strategically targeted framework for dual-use R&I to reduce strategic dependencies and enhance technological sovereignty within the EU and its partnership with NATO. It advocates for a "dual-use by design" approach, which encourages developers to anticipate cross-sectoral applications from the outset, ensuring that technological advances in fields like quantum and aerospace are robust and future-proof. The document highlights that such integration must be balanced with ethical and security assessments to prevent military misuse, aligning with broader EU values of transparency and fundamental rights while ensuring that R&D activities effectively support both commercial competitiveness and regional security.

[75] 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

[76] WHITE PAPER On options for enhancing support for research and development involving technologies with dual-use potential COM(2024) 27 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0027

8. Defense and artificial intelligence. European Parliament Briefing (April 2025).[77]

Relevance: The European Parliamentary Research Service (EPRS) briefing, "Defence and artificial intelligence", underscores the transformative role of Artificial Intelligence (AI) in modern warfare, particularly in intelligence gathering, autonomous systems, and cyber operations. While the EU AI Act explicitly excludes AI systems used solely for military, defense, or national security purposes, the document emphasizes its significant influence on dual-use technologies (e.g., drones) and its potential to shape future global debates on military AI regulation. The briefing identifies AI as a critical priority for EU-NATO cooperation, aimed at improving interoperability and safeguarding against threats from adversarial AI while adhering to NATO's Principles of Responsible Use.

Regarding implementation and ethics, the EPRS stresses the urgent need for robust AI-powered cybersecurity measures to address hybrid threats and protect critical infrastructure. It highlights the European Parliament's call for a comprehensive EU framework that aligns with international law and ensures meaningful human control over lethal autonomous weapons (LAWS). While the document does not explicitly detail "GDPR" or specific "Privacy by Design" technicalities, it emphasizes a human-centric, risk-based approach to AI governance, advocating for ethical guidelines, accountability, and transparency in deployment across both public administration and military operations to uphold democratic values and fundamental rights.

B. General AI Strategy & Interpretation

1. Coordinated Plan on AI (2021 Review)[78]

Relevance: The European Commission Coordinated Plan on Artificial Intelligence emphasizes "AI for the Public Sector" (including law enforcement).

It outlines a comprehensive EU framework for developing human-centric and trustworthy AI, emphasizing that compliance with the GDPR and data protection legislation is a prerequisite for AI development and data sharing. It highlights the Commission's proposal for the Artificial Intelligence Act, a horizontal regulatory framework that adopts a risk-based approach to safety and fundamental rights, distinguishing between high-risk and lower-risk AI systems.

To ensure AI ethics and security, the plan integrates the "Ethics Guidelines for Trustworthy AI" developed by the High-Level Expert Group, promoting principles such as ethics by design, and technical robustness. Regarding cybersecurity, the document aligns with the EU Cybersecurity Strategy and involves ENISA to address AI-specific threats, proposing "Security Operation Centres" to detect malicious activities.

Regarding NATO and the domain of defense, the document explicitly states that the Coordinated Plan does not address the development and use of AI for military purposes. Consequently, there are no provisions related to NATO cooperation. However, in the area of dual-use goods, the text notes the revision of the Dual-Use Regulation to ensure accountability and transparency in the trade of sensitive technologies. It also briefly references the "Action Plan on Synergies between civil, defence and space industries" in the context of critical technologies and robotics, but the primary focus remains strictly on civil applications, specifically excluding military AI from this specific plan.

2. Commission Guidelines on Prohibited AI Practices (Feb 2025)[79]

[77] Defense and artificial intelligence. European Parliament Briefing (April 2025) https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

[78] European Commission Coordinated Plan on Artificial Intelligence 2021 Review. https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

[79] 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

Relevance: Non-binding but critical guidance on interpreting the "unacceptable risk" categories (e.g., remote biometric identification). These interpretations are vital for dual-use vendors (e.g., camera/drone manufacturers) to know when a police use-case crosses the line into a ban.

These guidelines provide an overview of AI practices that are deemed unacceptable due to their potential risks to European values and fundamental rights. The guidelines specifically address practices such as harmful manipulation, social scoring, and real-time remote biometric identification, among others.

The guidelines are designed to ensure the consistent, effective, and uniform application of the AI Act across the European Union. While they offer valuable insights into the Commission's interpretation of the prohibitions, they are non-binding, with authoritative interpretations reserved for the Court of Justice of the European Union (CJEU). The guidelines provide legal explanations and practical examples to help stakeholders understand and comply with the AI Act's requirements. This initiative underscores the EU's commitment to fostering a safe and ethical AI landscape.

3. European Commission. European approach to artificial intelligence, policy review (2025)[80].

Relevance: The European approach to artificial intelligence - European Commission relevant policy review - outlines a comprehensive strategy focused on excellence and trust, aiming to make the EU a global leader in AI while safeguarding democratic values and fundamental rights. A key provision is the EU AI Act, which introduces a risk-based regulatory framework to ensure that AI systems used in the Union are safe, transparent, and human-centric. While the document primarily focuses on commercial and public sector AI (e.g., healthcare, education), it underscores that building high-performance, robust systems requires high-quality data, which is supported by broader initiatives like the EU Cybersecurity Strategy and the Data Union Strategy.

Regarding implementation, the page details the AI Continent Action Plan (April 2025) and the Apply AI Strategy (October 2025), which focus on large-scale computing infrastructure and AI adoption in strategic industrial ecosystems. Although the text does not explicitly detail technical provisions for "NATO" or the "defense" sector, it emphasizes technological sovereignty and the need for trustworthy AI that complies with established ethics and security standards, such as the General-Purpose AI (GPAI) Code of Practice. The strategy reflects a commitment to "Security and Privacy by Design" by establishing the European AI Office to oversee the implementation of the AI Act and by launching tools like the AI Act Service Desk to provide legal clarity for businesses across all sectors.

4. AI Continent Action Plan (April 2025)[81]

Relevance: Based on the "AI Continent Action Plan" (COM(2025) 165), the relevant provisions focus heavily on the implementation of the EU AI Act to create a single market for trustworthy and human-centric AI, establishing support structures like the AI Office and an AI Act Service Desk to assist with regulatory compliance. While the document does not explicitly detail "privacy by design" or "security by design" principles, it confirms that the AI Act will function alongside existing legislation such as the GDPR (referenced regarding the interplay of laws) and emphasizes strict safeguards for data security, confidentiality, and integrity within the upcoming Data Union Strategy.

Regarding defense and dual-use domains, the plan explicitly identifies "security and defence" as a key sector for the "Apply AI Strategy," noting that foundational AI technologies are critical inputs for both economic growth and military pre-eminence. The document also highlights the GenAI4EU initiative, which funds applied research to enhance cyber-defence capabilities. However, the document does not reflect provisions related to NATO cooperation.

[80] European Commission. European approach to artificial intelligence, policy review (2025). https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[81] The AI Continent Action Plan. https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan

5. Apply AI Strategy (October 2025)[82]

Relevance: The Commission Communication COM(2025) 723, titled "Apply AI Strategy," sets out a sectoral framework to accelerate the adoption of trustworthy Artificial Intelligence (AI) across 10 key industrial and public sectors, including healthcare, energy, and notably, defence, security, and space. Building on the EU AI Act, the strategy emphasizes the creation of "sectoral flagships" to boost competitiveness while upholding principles of non-discrimination and human-centric design. It specifically addresses dual-use AI by proposing workshops to discusión synergies between civilian and defense experts, aiming to establish a common understanding of the state of the art and facilitate the trusted integration of AI into both domains.

Regarding implementation, the strategy reinforces "Security and Privacy by Design" through the establishment of AI Testing and Experimentation Facilities and the launch of the AI Act Service Desk to support legal compliance. It details a commitment to cybersecurity by funding projects that use AI for threat detection, vulnerability analysis, and incident recovery. While the document focuses on innovation and technological sovereignty, it underscores the necessity of adhering to GDPR and data protection laws, proposing targeted measures to allow the processing of special categories of personal data for bias detection, provided that appropriate safeguards are in place. This comprehensive approach aims to position the EU as an "AI Continent" while ensuring that all AI applications are safe, ethically grounded, and resilient against hybrid threats.

3.3. Relevant European Court of Justice (CJEU/ECJ) Cases

While no case has yet ruled on the EU AI Act itself, the following judgments establish the legal "red lines" for automated processing, national security exemptions, and data rights that will dictate how the AI Act is enforced in dual-use contexts.

A. Limits of "National Security" Exemptions

1. La Quadrature du Net (Joined Cases C-511/18, C-512/18, etc.) (2020)[83]

Relevance: The Court ruled that Member States cannot cite "national security" to issue blanket mandates for mass data retention. This is crucial for the AI Act's dual-use scope: it prevents governments from easily labeling a civilian AI surveillance tool as "national security" just to bypass EU regulations.

The Court of Justice of the European Union (CJEU) ruling in Joined Cases C-511/18, C-512/18, and C-520/18 (La Quadrature du Net and Others) reaffirms that EU law-specifically the ePrivacy Directive (2002/58) read in light of the Charter of Fundamental Rights-precludes national legislation that mandates the "general and indiscriminate" retention of traffic and location data for the purpose of combating crime. However, the Court establishes a critical exception for national security: when a Member State faces a "genuine and present or foreseeable" serious threat to its national security, it may temporarily order the general retention of such data. This preventive measure must be strictly limited in time and subject to effective review by a court or an independent administrative body to prevent abuse.

Regarding implementation and dual-use scenarios, the ruling clarifies that even in the context of national security, data retention cannot be systematic or continuous. The Court allows for the automated analysis and real-time collection of data only when a serious threat is shown to exist, provided that the criteria for analysis are specific, reliable, and non-discriminatory-explicitly prohibiting criteria based on sensitive attributes like racial origin, political opinions, or religious beliefs. Furthermore, the judgment underscores that while combating serious crime and safeguarding public security are vital objectives, they do not justify the same level of interference as national security; for these purposes, only targeted retention

[82] 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

[83] C-511/18 - La Quadrature du Net and Others. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

(based on specific geographical areas or groups of persons) or the "expedited retention" (quick-freeze) of data is permissible under EU privacy and GDPR standards.

2. Ligue des droits humains (Case C-817/19) (2022)[84]

Relevance: Concerned the processing of PNR (passenger name record) data. The Court held that automated processing systems must have reliable, non-discriminatory criteria and human review. This sets the judicial standard for the "Human Oversight" requirements in the AI Act.

The CJEU ruling in Case C-817/19 (Ligue des droits humains), delivered on June 21, 2022, addresses the validity and interpretation of the Passenger Name Record (PNR) Directive (2016/681) in light of the Charter of Fundamental Rights. The Court upheld the Directive but imposed strict limitations on its implementation to ensure that the processing of passenger data is limited to what is "strictly necessary" for combating terrorism and serious crime. A central provision is the prohibition of the general and indiscriminate collection of PNR data for intra-EU flights; such measures are only permissible if a Member State establishes a "genuine and present or foreseeable" terrorist threat. In the absence of such a threat, PNR processing for domestic flights must be restricted to specific routes or airports based on objective risk criteria.

Regarding national security and data protection, the ruling clarifies that the PNR regime cannot be extended to ordinary crime and must adhere to high standards of personal data protection and the GDPR. The Court explicitly forbids the use of artificial intelligence (AI) in the form of self-learning systems ("machine learning") for the automated advance assessment of passengers, as the opacity of such systems could deprive individuals of their right to an effective judicial remedy. Furthermore, the judgment mandates that any automated match must be subject to an individual human review before any action is taken. Passenger data must generally be deleted after six months unless a concrete connection to a security risk is established, ensuring that the surveillance regime does not evolve into a "digital panopticon" without proper oversight.

3. VD and SR. (Joined Cases C-339/20, C-397/20) (2020)[85]

Relevance: The Court of Justice of the European Union (CJEU) ruling in Joined Cases C-339/20 and C-397/20 (VD and SR), delivered on September 20, 2022, confirms that EU law-specifically the ePrivacy Directive (2002/58) read in light of the Charter of Fundamental Rights-precludes national legislation that mandates the general and indiscriminate retention of traffic and location data for the purpose of combating market abuse, such as insider dealing. The case arose after the French Financial Markets Authority (AMF) prosecuted two individuals using telephone call records obtained under French law, which required operators to retain such data for one year. The Court reaffirmed its established jurisprudence that such broad retention constitutes a serious interference with the rights to privacy and personal data protection, even when the objective is to investigate serious economic crimes.

Regarding the legal implications and national security, the judgment clarifies that a national court cannot restrict the temporal effects of a declaration of invalidity regarding such legislation. While the Court acknowledges that the Market Abuse Regulation and Directive grant authorities the power to access existing records, these powers must be interpreted in accordance with the GDPR and the ePrivacy Directive, which limit data retention to what is strictly necessary. The ruling highlights that general and indiscriminate retention is permissible only in the event of a serious and current threat to national security. In contrast, for the investigation of serious crime or market abuse, only targeted retention (based on specific categories of persons or geographical areas) or the "quick freeze" (expedited retention) of specific data is considered proportionate and lawful under Union law.

B. Automated Decision-Making (The "Black Box" Precedents)

[84] C-817/19 - Ligue des droits humains. https://curia.europa.eu/juris/liste.jsf?num=C-817/19
[85] Joined Cases C-339/20, C-397/20 - VD and SR. https://curia.europa.eu/juris/liste.jsf?num=C-339/20&language=en

1. SCHUFA Holding AG (Case C-634/21) (Dec 2023)[86]

Relevance: Ruled that a credit score generated by an algorithm constitutes an "automated decision" under GDPR if it decisively influences the outcome. This prevents AI providers from hiding behind the claim that their tool is "just a recommendation," forcing dual-use tools (e.g., risk assessment software) to comply with strict transparency rules.

The Court of Justice of the European Union (CJEU) ruling in SCHUFA Holding AG (Case C-634/21), delivered on December 7, 2023, establishes that the automated generation of a credit score by a credit reference agency (CRA) constitutes "automated individual decision-making" under Article 22(1) of the GDPR if a third party (such as a bank) relies heavily on that score to make a final decision. The Court rejected SCHUFA's argument that it only provides "preparatory acts" and that the actual decision is made by the lender; instead, it found that when a poor score leads "in almost all cases" to the refusal of a loan, the establishment of the score itself is the de facto decision. This interpretation aims to prevent a "legal gap" where neither the CRA nor the lender would be fully responsible for explaining the logic behind the automated process to the data subject.

The ruling has significant implications for AI security and ethics, as it clarifies that any organization providing automated risk-based scores-including those for identity verification or fraud detection-may be subject to the strict requirements of Article 22. Under this provision, such automated decisions are generally prohibited unless they are necessary for a contract, authorized by law, or based on explicit consent, and they must always be accompanied by safeguards such as the right to human intervention and the right to an explanation. Additionally, in the joined cases C-26/22 and C-64/22, the Court ruled that private agencies like SCHUFA cannot lawfully retain data from public insolvency registers (such as a "discharge from remaining debt") for longer than the six-month period provided for in the public register, as doing so constitutes an unjustifiable interference with the data subject's right to be forgotten and their ability to participate in economic life.

2. Dun & Bradstreet Austria GmbH (Case C-203/22) (Feb 2025)[87]

Relevance: Established that individuals have a right to know the "logic involved" in an automated decision, and that trade secrets cannot be used as a blanket refusal to explain how an AI system works. This directly impacts providers of high-risk dual-use AI who might try to hide their algorithms.

The CJEU ruling in Dun & Bradstreet Austria GmbH (Case C-203/22), delivered on February 27, 2025, significantly bolsters the "right to an explanation" under Article 15(1)(h) of the GDPR in the context of automated individual decision-making. The Court clarified that when an individual is subjected to an automated decision with legal or significant effects (such as the refusal of a mobile phone contract based on a credit score), they are entitled to receive "meaningful information about the logic involved". This means the data controller must provide a sufficiently detailed and intelligible explanation of the procedures and principles applied, enabling the person to understand how their personal data influenced the result and to challenge its accuracy.

A key provision of the ruling addresses the tension between transparency and proprietary interests: the Court held that trade secrets and intellectual property rights cannot be used as a blanket defense to withhold information from the data subject. If a company claims that full disclosure would compromise its "secret sauce" (e.g., a proprietary algorithm), it must still submit the allegedly protected information to a court or supervisory authority. This body must then conduct a case-by-case balancing exercise to determine the extent of the access right, ensuring that the protection of business secrets does not effectively nullify the individual's fundamental right to verify the lawfulness of their data processing. While the Court noted that disclosing the complex algorithm itself may not be necessary-or even helpful-to the consumer, it mandated that the explanation must at least set out the "key parameters" and the extent to which variations in the data would have led to a different outcome.

[86] Case C-634/21 - SCHUFA Holding AG. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
[87] Case C-203/22 - Dun & Bradstreet Austria GmbH. https://curia.europa.eu/juris/liste.jsf?num=C-203/22

C. Emerging AI Liability & Copyright

3. Case C-250/25 (Pending, 2025)[88]

Relevance: The first referral specifically addressing Generative AI and Copyright (training data scraping). While primarily civil, the ruling will determine the liability of General Purpose AI models, which are inherently dual-use.

The pending case Like Company v. Google Ireland Ltd. (Case C-250/25), referred by the Budapest Metropolitan Court in April 2025, represents the first preliminary ruling request to the CJEU specifically addressing the intersection of generative AI and EU copyright law. The dispute centers on whether Google's chatbot, Gemini, infringed the rights of the Hungarian news publisher Like Company by generating detailed summaries of its copyright-protected articles without authorization. A central provision at issue is Article 15 of the CDSM Directive (2019/790), which grants press publishers the right to control online uses of their content beyond "very short extracts". The Court is asked to determine if displaying AI-generated summaries that mirror original content constitutes a "communication to the public" and whether the act of training a Large Language Model (LLM)-which involves tokenization and pattern recognition-amounts to an act of reproduction under Article 2 of the InfoSoc Directive.

The ruling's implications for AI security and ethics are profound, as it will clarify whether commercial LLM training on publicly available content falls under the Text and Data Mining (TDM) exception (Article 4 of the CDSM Directive) or whether such use is invalidated by its commercial nature and the economic harm caused to original rightsholders. If the CJEU rules in favor of the publisher, AI developers may be forced to obtain licences for both training and deployment in Europe, significantly increasing operational costs and potentially reshaping the development of dual-use AI technologies. Conversely, a ruling for Google could expand the scope of the TDM exception, allowing for broader "transformative" uses of data without compensation. While this case is primarily a copyright matter, it reflects the broader EU priority of ensuring that technological progress remains anchored in fundamental rights and a fair balance between innovation and the protection of original creative works.

3.4. National sources of the Republic of Lithuania

Lithuania, being both a NATO member and an active EU state, is forced to quickly and consistently integrate the policies of these organizations into its national system, especially in the field of dual-use (civilian and military) technologies. Lithuania's cybersecurity policy is one of the most developed in the Baltic region, closely integrating EU and NATO requirements. Below are the sources and initiatives of Lithuania's national policy. Although the purpose of this document is not to examine the legal acts at the legislative level, the laws mentioned here help to better define the overall picture of policy initiatives and the extent of progress in a broader context.

3.4.1. Cybersecurity (Transposition of the NIS2 Directive)

On 18 October 2024, a new version of the Law of the Republic of Lithuania on Cybersecurity[89] entered into force, which transposes the essential provisions of the EU NIS2 Directive into national law.

Meaning: to strengthen the resilience of public and private sector entities (operators of particularly important and critical services) to cyber threats. It establishes specific organizational and technical requirements for cybersecurity entities.

[88] Case C-250/25 - Like Company v. Google Ireland Ltd. https://curia.europa.eu/juris/liste.jsf?num=C-250/25

[89] Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr

Mechanism: The implementing legal acts (e.g., the National Cyber Incident Management Plan[90]) have been approved, and entities will be registered in the Cybersecurity Entity Register (CISE)[91], which is managed by the National Cybersecurity Center (NCSC).

Dual Purpose: The Ministry of National Defense (MND) and the NCSC subordinate to it are the main institutions that form and coordinate the state's cybersecurity policy. Their activities include strengthening the state's cybersecurity and defense capabilities, which directly includes the military sphere.

3.4.2. Data Protection (GDPR) and National Security

Lithuanian policy clearly distinguishes between the processing of personal data for civilian (under the GDPR) and defense/national security (under special laws) purposes, but maintains consistency.

A. Integrating GDPR into AI

The State Data Protection Inspectorate (SDI) provides detailed guidelines[92] on the use of AI systems, emphasizing the application of GDPR principles (lawfulness, data minimization, accountability).

Practice: It is emphasized that organizations (including the public sector) must conduct a Risk Assessment and, in case of high risk, a Data Protection Impact Assessment (DPIA) before implementing AI systems, ensuring Transparency and informing individuals about the use of AI.

B. Data Processing in the National Security System

The Ministry of National Defence (MND) and the Lithuanian Armed Forces have separate rules for the processing of Personal Data.

Legal Basis: Personal data is processed for national security and/or defence purposes, in accordance with specific laws (e.g. the Law on Personal Data Processed for Law Enforcement or National Security Purposes[93]), which are in line with the EU Directive on the Processing of Personal Data for Law Enforcement Purposes, and not directly with the GDPR (although the general principles are maintained).

3.4.3. Artificial Intelligence (AI) and Dual Purpose (AI Act)

Lithuania aims to develop the AI industry, while ensuring its security and ethics, closely following the EU AI Act.

Lithuanian Artificial Intelligence Strategy[94]. The Strategy (prepared by the Ministry of Economy and Innovation) promotes the development and deployment of AI in key sectors, recognizing AI systems as systems that demonstrate intelligent and intelligent behavior.

The Ministry of National Defence (MND) has initiated activities to examine the possibilities of implementing AI in the national defence system (plans for 2025). This shows an active readiness to integrate the provisions of the DI Act into dual-use technologies that are not exclusively military.

Funding for Defence and Security Technologies: The Government and the Ministry of Economy and Innovation allocate significant funding (e.g. through the European Strategic Technology Platform – STEP) for the development and production of defence and security technologies. This is a direct promotion of dual-use

[90] National Cyber Incident Management Plan of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

[91] Cybersecurity Entity Register (CISE). https://www.nksc.lt/ksis

[92] The State Data Protection Inspectorate of the Republic of Lithuania. Guidelines. https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/work/

[93] Law on Personal Data Processed for Law Enforcement or National Security Purposes of the Republic of Lithuania https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.397419/asr

[94] Lithuanian Artificial Intelligence Strategy. https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf

technologies, focused on technological sovereignty in the EU context. This support is directed at companies developing innovations that will be used in both the civilian and military sectors.

Relationship with NATO: Lithuanian policy consistently emphasizes the National Security Interest – the vitality and unity of NATO and the EU. Lithuania's participation in international countermeasures (e.g. coordinated EU and NATO statements on attributing cyber attacks to hostile states) demonstrates full support for NATO's policy of collective defence and counter-cyber measures.

In summary, Lithuanian policy is adaptive and integrative: it actively transfers EU regulation (NIS2, GDPR, AI Act) to the field of civilian and hybrid threats, and the National Defence System oversees the use of these technologies and data for defense and national security purposes through special national legal acts, taking into account NATO principles.

Conclusions

1. Policy conclusions

A. Convergence of Legal and Ethical Frameworks

- The boundary between civilian and military technology is increasingly blurred. While the EU AI Act (August 2024) and the NATO Revised AI Strategy (July 2024) operate in different jurisdictions, they have converged on a "Human-Centric" and "Risk-Based" approach. The EU's "High-Risk" classification mirrors NATO's focus on "Critical Use Cases," both requiring stringent robustness, traceability, and human oversight.

B. The Dual-Use Regulatory Gap

- A significant "governance gap" exists for dual-use AI. The EU AI Act explicitly excludes systems used *exclusively* for military purposes, but it applies to dual-use technologies sold on the civilian market. This creates a "Brussels Effect" where defense contractors must adhere to civilian standards (GDPR, AI Act, NIS2) to maintain market access, effectively setting a de-facto technical baseline for military applications.

C. Security & Privacy by Design as a Strategic Necessity

- "Security by Design" (under NIS2 and the Cyber Resilience Act) and "Privacy by Design" (under GDPR) are no longer just compliance checkboxes; they are now viewed as fundamental to Strategic Autonomy. For Lithuania and the wider Alliance, the integrity of the data supply chain is recognized as a primary defense vulnerability.

2. Functional conclusions

A. The "Dual-Use" Regulatory Trap

- The EPMwDC project operates in a complex "omni-use" or dual-use environment. While the product addresses a gap in espionage prevention, it faces a bifurcated legal landscape. The EU AI Act applies strictly to any dual-use system that enters the civilian market (e.g., banking, private enterprise), while NATO policies and national defense laws govern its use in purely military contexts. Relying solely on a "national security" exemption to bypass EU regulations is risky, as the CJEU has ruled that such exemptions must be temporary and specifically justified, prohibiting blanket mass surveillance.

B. Mandatory "By Design" Requirements

- Both EU and NATO frameworks demand that security and ethics be engineered into the product from the start, not added as an afterthought. EU Context: The Cyber Resilience Act and NIS2 Directive (transposed in Lithuania) require strict cybersecurity standards for hardware and software products. NATO Context: The Alliance mandates "Security by Design" and alignment with the Principles of Responsible Use (PRUs), specifically regarding reliability, governability, and bias mitigation.

C. Algorithmic Transparency and Liability

- Recent CJEU rulings establish that companies cannot hide behind "trade secrets" to refuse explaining how an AI decision was reached, especially if that decision significantly affects an individual (e.g., an accusation of espionage). Furthermore, automated systems cannot serve as the sole basis for legal decisions; human oversight is legally required to prevent "black box" liability.

3. Strategic Recommendations

A. For Policy Makers & Government Institutions

- Harmonize Impact Assessments: Streamline the overlap between DPIA (Data Protection Impact Assessments) and the new FRIA (Fundamental Rights Impact Assessments) for dual-use AI to prevent administrative fatigue for tech innovators.
- Enhance "Sandboxing": Expand the Innovation Agency's AI Sandbox specifically for dual-use startups, providing them with legal "safe harbors" to test AI models in real-world conditions without early-stage penalty risks.

B. For Defense and Security Organizations

- Adopt "Omni-Use" Data Governance: Transition from a "Need-to-Know" to a "Need-to-Share" data-centric model, ensuring that data used for AI training remains compliant with GDPR principles (anonymization/pseudonymization) while maintaining military utility.
- Implement Active Cyber Protection: Consistent with Lithuania's push for Deterrence by Denial, integrate AI-driven active defense mechanisms that comply with NIS2's reporting requirements but operate at machine speed.

C. For Industry and Dual-Use Developers

- Technical Documentation as a Product: Treat the Technical Documentation (Annex IV of AI Act) as a core product feature. Systems that are "explainable by design" will find faster procurement paths in both the EU civilian market and NATO defense contracts.
- Adversarial AI Testing: Prioritize testing against Data Poisoning and Model Manipulation. Resilience to these attacks is now a mandatory requirement for "High-Risk" systems under the AI Act (Art. 15) and a key "Reliability" principle for NATO.

4. Summary of Integrated Governance

Domain	EU Requirement (Civilian)	NATO Principle (Defense)	Recommendation for Alignment
Accountability	Human Oversight (Art. 14)	Responsibility & Accountability	Ensure a "Human-in-the-Loop" for all critical decision-support tools.

Security	Cybersecurity (NIS2/Art. 15)	Reliability & Governability	Implement a single "Security-by-Design" architecture for both markets.
Ethics	Fundamental Rights Impact	Bias Mitigation	Use diverse, synthetic datasets to train models while protecting privacy.
Data	GDPR Compliance	Lawfulness & Traceability	Maintain a rigorous "Data Pedigree" (provenance) for all training sets.

Annex - Dual-Use AI Compliance Checklist

1. Classification & Scope (The "Strategic Filter")

- Identify Dual-Use Status: Determine if your system is exclusively military (exempt from AI Act but subject to NATO PRUs) or "Dual-Use" (subject to AI Act if placed on the civilian market).
- Determine Risk Level (EU AI Act): Categorize your system as Prohibited, High-Risk (e.g., biometrics, critical infrastructure), Limited, or Minimal risk.
- Define Legal Role: Are you the Provider (developer), Deployer (user), or Importer? Your obligations change significantly based on this.

2. Governance & Ethics (NATO/EU Alignment)

- Implement "Meaningful Human Control": Design human-machine interfaces that allow for "Governability" (NATO) and "Human Oversight" (EU AI Act, Art. 14).
- Establish Bias Mitigation: Perform proactive audits on datasets to minimize discrimination (GDPR/NATO) and ensure "Data Governance" (AI Act, Art. 10).
- Establish a DARB-Ready File: Prepare a "Responsibility Folder" that documents how your system aligns with NATO's 6 PRUs, which can be presented during defense procurement.

3. Privacy & Data Protection (GDPR/Security by Design)

- Privacy by Design: Ensure data minimization and anonymization are embedded in the model training phase.
- DPIA & FRIA: Conduct a Data Protection Impact Assessment (GDPR) and a Fundamental Rights Impact Assessment (AI Act) for high-risk systems.
- Cybersecurity Compliance (NIS2/Lithuania): Register in the Kibernetinio saugumo subjektų registras if applicable and implement technical measures within the 24-month grace period.

4. Technical Reliability & Security

- Adversarial Testing: Conduct "Red Teaming" to test resilience against data poisoning and model evasion (AI Act, Art. 15).
- Automatic Logging: Ensure the system records events for "Traceability" (NATO) and "Record-Keeping" (AI Act, Art. 12).
- Technical Documentation: Maintain a live "EU Declaration of Conformity" and detailed architecture maps for national regulators (NKSC/VDAI).

References

1. NATO's Strategic Warfare Development Command. Digital Transformation. https://www.act.nato.int/activities/digital-transformation/#:~:text=In%20October%202021%2C%20NATO%20Defence,and%20commitment%20to%20international%20law
2. NATO sets a Standard for Ethical Use of New Technologies, News, European Commission. https://ec.europa.eu/newsroom/cipr/items/722501/en#:~:text=The%20upcoming%20adoption%20of%20NATO's,will%20follow%20the%20same%20approach.
3. NATO AI Strategy (endorsed October 202; revised July 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
4. NATO 2022 Strategic Concept. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf
5. "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
6. 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
7. NATO's Data and Artificial Intelligence Review Board (DARB) https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/natos-data-and-artificial-intelligence-review-board
8. Autonomy Implementation Plan (October 2022). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/summary-of-natos-autonomy-implementation-plan
9. NATO's Digital Transformation Implementation Strategy (October 2024). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/17/natos-digital-transformation-implementation-strategy
10. Defence Innovation Accelerator for the North Atlantic (DIANA). https://www.diana.nato.int/
11. The NATO Innovation Fund. https://www.nif.fund/
12. R. Powel. The EU AI Act: National Security Implications. Centre for Emerging Technology and Security (August 2024). https://cetas.turing.ac.uk/sites/default/files/2024-07/cetas_explainer_-_the_eu_ai_act_-_national_security_implications.pdf
13. S. Kulueva, A. Grigoriescu (ed.). Blind Spots in AI Governance: Military AI and the EU's Regulatory Oversight Gap. ES Think Tank (October 2025). https://esthinktank.com/2025/10/03/blind-spots-in-ai-governance-military-ai-and-the-eus-regulatory-oversight-gap/#:~:text=Accordingly%2C%20while%20the%20Regulation%20excludes,responsibility%20of%20each%20member%20state
14. Review of the EU Artificial Intelligence Act. https://artificialintelligenceact.eu/article/2/#:~:text=Summary,or%20fall%20under%20certain%20articles
15. European Commission Press corner - Questions and answers regarding Artificial intelligence (August 2024). https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683
16. European Policy centre. From Dual-Use to Omni-Use: Securing Europe's Future (October 2025). https://www.epc.eu/publication/from-dual-use-to-omni-use-securing-europes-future/
17. Centre for Future Generations. "Double-edged tech: Advanced AI & compute as dual-use technologies" (2025). https://cfg.eu/double-edged-tech/#:~:text=The%20US%20Executive%20Order%20on%20the%20Safe%2C%20Secure%2C%20and%20Trustworthy,cases%20such%20as%20weapon%20generation
18. The Leupold Legal. "Does the EU AI Act jeopardize Europe's defense readiness?" (November 2025). https://leupoldlegal.com/does-the-eu-ai-regulation-jeopardize-europes-defense-

readiness/#:~:text=Although%20it%20has%20been%20pointed,it%20already%20complies%20with%20it

19. Gregory Smith, Karlyn D. Stanley, Krystyna Marcinek, Paul Cormarie, Salil Gunashekar.General-Purpose Artificial Intelligence (GPAI) Models and GPAI Models with Systemic Risk: Classification and Requirements for Providers (August 2024). https://www.rand.org/pubs/research_reports/RRA3243-1.html
20. 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
21. Roadmap on critical technologies for security and defence COM(2022) 61 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0061
22. White Paper on Export Controls COM(2024) 25 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025
23. EU Strategic Compass for Security and Defence. https://www.consilium.europa.eu/en/policies/strategic-compass/
24. Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council - "Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence (2025). https://data.consilium.europa.eu/doc/document/ST-8023-2025-INIT/en/pdf
25. 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
26. WHITE PAPER On options for enhancing support for research and development involving technologies with dual-use potential COM(2024) 27 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0027
27. Defense and artificial intelligence. European Parliament Briefing (April 2025) https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf
28. European Commission Coordinated Plan on Artificial Intelligence 2021 Review. https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review
29. 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
30. European Commission. European approach to artificial intelligence, policy review (2025). https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
31. The AI Continent Action Plan. https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan
32. 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
33. C-511/18 - La Quadrature du Net and Others. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
34. C-817/19 - Ligue des droits humains. https://curia.europa.eu/juris/liste.jsf?num=C-817/19
35. Joined Cases C-339/20, C-397/20 - VD and SR. https://curia.europa.eu/juris/liste.jsf?num=C-339/20&language=en
36. C-634/21 - SCHUFA Holding AG. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
37. C-203/22 - Dun & Bradstreet Austria GmbH. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
38. C-250/25 - Like Company v. Google Ireland Ltd. https://curia.europa.eu/juris/liste.jsf?num=C-250/25
39. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
40. National Cyber Incident Management Plan of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
41. Cybersecurity Entity Register (CISE). https://www.nksc.lt/ksis

42. The State Data Protection Inspectorate of the Republic of Lithuania. Guidelines. https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/work/
43. Law on Personal Data Processed for Law Enforcement or National Security Purposes of the Republic of Lithuania https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.397419/asr
44. Lithuanian Artificial Intelligence Strategy. https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf
45. Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
46. The Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847
47. NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
48. Krol, LLC: https://www.kroll.com/en/about-us
49. Berkeley Research Group, LLC: https://www.thinkbrg.com/
50. B.C. Strategy, Ltd: https://www.blackcube.com/
51. Information Commissioner's Office. https://ico.org.uk/
52. Competition and Markets Authority. https://www.gov.uk/government/organisations/competition-and-markets-authority
53. Financial Conduct Authority. https://www.fca.org.uk/
54. Data (Use and Access) Act 2025. https://www.legislation.gov.uk/ukpga/2025/18/contents
55. Digital Markets, Competition and Consumers Act 2024. https://www.legislation.gov.uk/ukpga/2024/13/contents
56. Executive Order 14179 of January 23, 2025. Removing Barriers to American Leadership in Artificial Intelligence. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
57. Executive Order "Ensuring a National Policy Framework for Artificial Intelligence". https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/
58. SB-53 Artificial intelligence models: large developers. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53
59. SB-942 California AI Transparency Act. https://www.leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942
60. SB24-205 Consumer Protections for Artificial Intelligence. https://leg.colorado.gov/bills/sb24-205
61. The Texas Responsible AI Governance Act. https://www.nortonrosefulbright.com/en/knowledge/publications/c6c60e0c/the-texas-responsible-ai-governance-act
62. The Investigatory Powers Act 2016. https://www.legislation.gov.uk/ukpga/2016/25/contents
63. Biometric Information Privacy Act (BIPA). https://www.aclu-il.org/campaigns-initiatives/biometric-information-privacy-act-bipa/
64. The "Genesis Mission" Executive Order (Nov 2025) https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/

Finansuoja Europos Sąjunga
NextGenerationEU
Mykolo Romerio universitetas
NAUJOS KARTOS LIETUVA

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