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: ***CTI-Balanced***

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

Action result: ***CTI-balanced GDPR-related Practices***

CTI-balanced GDPR-related Practices

Table of Contents

Introduction *3*
1. Guidelines on GDPR application *3*
2. Strategic Documents on Cybersecurity and Information Sharing *5*
3. Legal Precedents (Data Collection, "Mass Surveillance", CTI sharing) *8*
4. National practices in the Republic of Lithuania *10*
5. National practices in selected EU Member States *11*
Conclusions *14*
Recommendations *14*
References *16*

Introduction

Cyber threat intelligence-based Sector and National collective cybersecurity are relatively new phenomenon. There are no well-tested methodologies, approaches, processes, procedures and automation for cyber threat intelligence management, thus, most countries are struggling in this domain with non-functioning solutions.

This document exclusively covers recent CTI-related data sharing on cyber incidents policy practices related to GDPR requirement implementation and challenges. The document includes a detailed overview of the recent policy practices in the European Union (EU), NATO, Lithuanian national jurisdiction and examples of relevant policy practices in several other EU Member States with regard to GDPR requirements.

1. Guidelines on GDPR application

An EDPB Guidance "Fundamentals of Secure AI Systems with Personal Data" (April 2025)[1] is a technical-legal guide on harmonizing AI security with GDPR requirements (data minimization, accuracy). This guidance is important for bridging the technical requirements of secure AI with the legal obligations of GDPR (Data Protection and Security). The Publication outlines a training curriculum for cybersecurity professionals working with personal data and artificial intelligence (AI) in the European Union (EU).

The document addresses information and societal threats primarily through its taxonomy of AI risks and ethical considerations. It identifies specific domains such as "Misinformation" and "Pollution of the information ecosystem," noting risks related to the spread of false information, the reinforcement of belief bubbles, and the "disinformation, surveillance, and influence at scale" conducted by malicious actors.

It highlights "Socioeconomic & environmental harms" as a key risk area, warning against power centralization, increased inequality, the devaluation of human effort, and "Discrimination & toxicity," which includes unfair treatment and exposure to toxic content.

Regarding psychological threats, the text explicitly references the EU AI Act's prohibition of AI systems that manipulate human behavior through "subliminal techniques" or exploit vulnerabilities based on age or disability to impair decision-making. It also warns of the "Loss of human agency and autonomy" and "Overreliance" on automated systems. While the specific term "hybrid threats" is not defined, the document covers overlapping concerns under "Malicious actors & misuse," describing the use of AI for cyberattacks, weapon development, and mass harm, which are components often associated with hybrid warfare strategies.

Guidance for Risk Management of Artificial Intelligence systems. European Data Protection Supervisor (November 2025)[2] This Guidance aims to guide EUIs acting as data controllers in identifying and mitigating some of these risks. More specifically, they focus on the risk of non-compliance with certain data protection principles elicited in the EUDPR for which the mitigation strategies that controllers must implement can be technical in nature – namely fairness, accuracy,

[1] Fundamentals of Secure AI Systems with Personal Data. EDPB Guidance. April 2025. https://www.edpb.europa.eu/system/files/2025-06/spe-training-on-ai-and-data-protection-technical_en.pdf

[2] Guidance for Risk Management of Artificial Intelligence systems. European Data Protection Supervisor. November 2025. https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-11-11-guidance-risk-management-artificial-intelligence-systems_en

data minimisation, security and data subjects' rights. As such, the technical controls listed in this Guidance are by no means exhaustive, and do not exempt EUIs from conducting their own assessment of the risks raised by their specific processing activities. In doing so, it refrains from ranking their likelihood and severity.

EDPS guidance indicates that data controllers (in this case, the organizations using the plug-in) must conduct a Data Protection Impact Assessment (DPIA), especially when using AI. Therefore, the project should provide a template DPIA for its clients.

According to this document, hybrid threats are characterized by the convergence of cyber operations with physical acts of sabotage, such as the recruitment of individuals via social media for vandalism and arson, often orchestrated by state-aligned groups to destabilize EU society. Information threats, specifically Foreign Information Manipulation and Interference (FIMI), are a primary concern.

2. Strategic Documents on Cybersecurity and Information Sharing

Apply AI Strategy (October 2025)[3]. This strategy directly encourages the creation of tools that "detect anomalies" and "analyze incidents," aligning with the project's goals. It notes that such tools in the security sector will likely be classified as high-risk. If the system uses AI for threat analysis, you must ensure proper data governance. The Apply AI Strategy emphasizes that quality data is essential but must be handled according to "Privacy by Design" principles. Moreover, it is crucial to distinguish between civil and military use. If the system is dual-use, the AI Act regulations apply to its civil applications (e.g., for private companies), even if the same system is used for defense.

High-Risk Classification. According to the Apply AI Strategy and the AI Act, systems used in critical infrastructure or democratic processes (e.g., election protection) will likely be classified as high-risk. This means the plug-in will require conformity assessments, a risk management system, and human oversight.

Moreover, the document emphasizes "lawful and effective access to data" for security purposes. It also stresses the need for "secure, efficient, and reliable data sharing" and ensuring "safety is embedded by design", which implies adherence to data protection principles without citing specific GDPR articles.

The document introduces the "Security Action for Europe (SAFE)", which allows Member States to invest in "AI-powered equipment and cybersecurity". Additionally, the strategy aims to build an "AI toolbox dedicated to public administrations".

The Union Rolling Work Programme for certification[4]. The Union Rolling Work Programme for certification emphasizes that security measures must be integrated from the design phase. This includes data minimization, i.e., collecting only what is strictly necessary to identify a threat (e.g., headers rather than full packet content).

The document outlines the strategic priorities for European cybersecurity certification, emphasizing the critical interplay between voluntary certification schemes and the mandatory requirements of the Cyber Resilience Act (CRA). For a plug-in project, the source clarifies that obtaining a European cybersecurity certificate (at a "substantial" assurance level) can demonstrate a "presumption of conformity" with the CRA's strict requirements for products with digital elements. This creates a clear incentive to align a product development process with these schemes, particularly focusing on "security-by-design" and "security-by-default" principles, which require integrating security measures and vulnerability handling throughout the entire lifecycle of the software.

Significantly, the document identifies "Managed Security Services" (MSS), specifically including incident response, penetration testing, and security audits, as a key area for future certification. Since the project aims to create a "cyber threat management system," this upcoming extension of the Cybersecurity Act is directly relevant. Certifying service under this future scheme could prevent market fragmentation and allow to offer services across different EU member states without navigating divergent national rules.

[3] Apply AI Strategy (Communication from the Commission Artificial Intelligence for Europe) COM(2025) 723 final. https://eur-lex.europa.eu/resource.html?uri=cellar:194ae542-a421-11f0-97c8-01aa75ed71a1.0001.02/DOC_1&format=PDF

[4] Union Rolling Work Programme for European cybersecurity certification. https://ec.europa.eu/newsroom/dae/redirection/document/102292

The document also introduces the concept of "composability," which would allow a system to re-use existing certificates from its sub-components, thereby reducing the administrative burden and "double evaluation" efforts.

Finally, the source addresses the practical challenges of certifying rapidly evolving software by proposing "fixed-time evaluation" methodologies. This approach is designed for products that require frequent updates and is highlighted as particularly beneficial for SMEs, offering a more flexible and resource-efficient alternative to traditional, time-intensive certification processes. The document also stresses the importance of adopting a "Secure Development Lifecycle" (SDL) approach, recommending to identify and apply relevant standards (e.g., ISO/IEC 27034) early in the development to facilitate future compliance and certification.

Defence Readiness Roadmap 2030. JOIN(2025) 27 final[5]. This Roadmap provides clear objectives, milestones with concrete dates for deliverables, and indicators to track progress. It proposes European flagship where urgency is greatest, to focus efforts, in accordance with international commitments, including NATO targets. Therefore, project could serve as the software layer or a contributing sensor for this flagship initiative.

The Commission's Readiness Roadmap 2030 outlines a detailed action plan to strengthen the European defense sector. A central proposal is the creation of "European Readiness Flagships," such as the "Eastern Flank Watch," designed to establish a comprehensive border defense capability with advanced surveillance, drone, and precision strike systems. The roadmap provides a clear timeline of milestones, including the adoption of the European Defence Industry Programme (EDIP) by November 2025, the establishment of Tech Alliances for Defence by the end of 2025, the hosting of the first annual Defence Industrial Summit by mid-2026, and the reskilling of 200,000 employees for the defense industry by 2026.

Defence Readiness Omnibus. Simplification proposal to boost industrial readiness[6]. The European Commission has adopted the Defence Readiness Omnibus, a comprehensive package aimed at establishing a defence-readiness mindset across the European Union. This initiative lays the groundwork for facilitating up to EUR 800 billion in defence investments over the next four years, enabling Member States and industry to respond swiftly and effectively to growing threats. Implication: The strict GDPR/AI Act compliance burden may be streamlined for dual-use technologies that serve strategic defence interests. The "Defence Readiness Omnibus" aims to simplify intra-EU transfers and security of supply standards.

NATO's Data Exploitation Framework Policy[7] (DEFP) establishes a framework to ensure that NATO is able to leverage data as a strategic resource, and to address challenges to data exploitation identified by Allies and members of the NATO Enterprise. Its objective is to put into place an overarching, comprehensive approach to ensuring data is used responsibly and in line with core Alliance values, with a focus on improving the data exploitation capabilities across all levels in the military, civilian and political domains.

[5] Preserving Peace - Defence Readiness Roadmap 2030. JOIN(2025) 27 final. https://defence-industry-space.ec.europa.eu/document/download/9db42c04-15c2-42e1-8364-60afb0073e68_en?filename=Joint-Communication%20_Defence-Readiness-Roadmap-2030.pdf

[6] Defence Readiness Omnibus. Simplification proposal to boost industrial readiness. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-readiness-omnibus_en

[7] NATO's Data Exploitation Framework Policy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/11/23/summary-of-natos-data-exploitation-framework-policy

The vision is to achieve information superiority and data-driven decision making at all levels across the Alliance by fully leveraging the value of NATO generated, national, and publicly available data.

The approach to data exploitation will be underpinned by core Alliance values and by principles of responsible development and use reflecting shared values and consistent with applicable international law. These data exploitation efforts will be driven by a strong, collaborative culture which encourages sharing of data in secure, trusted, and reliable environments. Data exploitation expertise and tools will be made easily accessible to all.

The policy establishes a framework that treats data as a "shared, strategic asset" essential for achieving "information superiority" and data-driven decision-making, which directly validates project's objective to collect and analyze cyber threat information. It explicitly encourages the leveraging of "publicly available data" alongside national and NATO-generated data, supporting the plug-in's potential to aggregate open-source intelligence. The document sets a strategic goal to establish a "single logical environment" that is "secure and governed by design," mandating that developing system must prioritize interoperability and security architecture from the outset to be compatible with Alliance standards.

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[8] 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.

The document explicitly identifies Foreign Information Manipulation and Interference (FIMI) and hybrid strategies as critical security threats that "undermine our democracies, security, societies and lives". It confirms the active operational use of the EU FIMI Toolbox and the EU Hybrid Toolbox to protect democratic integrity, specifically citing successful interventions during the June 2024 European elections and the Moldovan referendum and elections in late 2024 against intensifying Russian destabilization efforts.

The report underscores that hybrid activities have expanded to include sabotage, cyberattacks, and the weaponization of information, necessitating a coordinated response.

The document also highlights the importance of the FIMI Information Sharing and Analysis Centre (FIMI ISAC), which serves as a platform to reinforce the analytical capabilities of civil society organizations in countering disinformation. Furthermore, the text emphasizes a "whole-of-society approach" to preparedness, linking civilian and military efforts to build resilience against these multifaceted risks, which directly validates the need for platforms capable of identifying bots and manipulation at scale.

[8] Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf

3. Legal Precedents (Data Collection, "Mass Surveillance", CTI sharing)

These are the most critical sources for determining what data (IP addresses, traffic data) can be collected. CJEU case law confirms that IP Addresses and Metadata are sensitive data. Their collection and sharing cannot be "mass and indiscriminate" unless there is a direct threat to national security. If the system is for civil use (enterprises, public sector), "quick freeze" principle must be applied (retaining data only when a specific suspicion of a cyber incident arises, rather than monitoring all users continuously).

La Quadrature du Net (C-511/18, etc.)[9] – his is a foundational ruling stating that Member States cannot mandate the general and indiscriminate retention of traffic and location data for preventive purposes unless there is a genuine threat to national security. For combating crime (including cybercrime), only targeted retention is permitted.

The Court ruled that Member States cannot cite "national security" to issue blanket mandates for mass data retention. The Court 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.

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.

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 (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.

SCHUFA Holding AG (C-634/21)[10] – this is vital if the system automatically assesses risk (e.g., scoring a network as "safe" or "unsafe"). The Court ruled that algorithmic scoring which determines decisions falls under GDPR Article 22 restrictions. If a risk score generated by the plug-in leads to significant consequences (e.g., blocking access), it constitutes automated decision-making, requiring human intervention options and stricter GDPR safeguards.

The Court 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 ruling 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

[9] C-511/18 - La Quadrature du Net and Others. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
[10] Case C-634/21 - SCHUFA Holding AG. https://curia.europa.eu/juris/liste.jsf?num=C-634/21

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.

EDPS v SRB (C-413/23 P)[11] – the CJEU case EDPS v SRB (C-413/23 P) clarified that pseudonymized data is not necessarily considered personal data in the hands of the recipient if the recipient does not have the means to re-identify the data subjects. This implies that when sharing information between EU institutions, the system should transmit data in a format that the recipient cannot easily link to a specific individual without additional information.

The dispute stems from a decision by the EDPS finding that the SRB failed to fulfill its obligations relating to the processing of personal data. This failure occurred during a procedure for granting compensation to shareholders and creditors of a banking institution following that institution's resolution.

The judgment focuses on the interpretation of Regulation (EU) 2018/1725, specifically addressing the Concept of 'personal data' (Article 3(1)), the Concept of 'pseudonymisation' (Article 3(6)), and the obligation to inform the data subject (Article 15(1)(d)) concerning the transmission of pseudonymised data to a third party.

Dun & Bradstreet (C-203/22)[12] – 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.

Deutsche Wohnen (C-807/21)[13] – the CJEU case Deutsche Wohnen (C-807/21) clarified that fines under GDPR are imposed only in cases of "intent or negligence." Therefore, the project architecture must enable users to prove they took all necessary security measures, protecting them from liability in the event of an unavoidable incident.

The interpretation of provisions of Regulation (EU) 2016/679 (General Data Protection Regulation or GDPR). Specifically, the ruling focused on the conditions for imposing administrative fines on a legal person, analyzing the concepts of 'controller' (Article 4(7)), the powers of supervisory authorities (Article 58(2)), and the imposition of administrative fines (Article 83). The Court interpreted Article 58(2)(i) and Article 83 of Regulation 2016/679, concluding two main points regarding administrative fines levied against controllers that are legal persons and undertakings.

Requirement of Identifying a Natural Person: Article 58(2)(i) and Article 83(1) to (6) of the GDPR must be interpreted as precluding national legislation which permits an administrative fine to be imposed on a legal person (in its capacity as controller) for an infringement (referred to in Article 83(4) to (6)) only if that infringement has previously been attributed to an identified natural person.

[11] C-413/23 P (EDPS v SRB). Pseudonymization and AI Model Training (GDPR). September 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

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

[13] C-807/21 (Deutsche Wohnen). GDPR Liability and Cyber-Fines. December 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=282192&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8123480

4. National practices in the Republic of Lithuania

Transposition of NIS2 Directive in Lithuania[14] - it provides the legal basis for information sharing regarding incidents between institutions. On 18 October 2024, a new version of the Law of the Republic of Lithuania on Cybersecurity entered into force, which transposes the essential provisions of the EU NIS2 Directive into national law.

It strengthens 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.

The implementing legal acts (e.g., the National Cyber Incident Management Plan[15]) have been approved, and entities will be registered in the Cybersecurity Entity Register (CISE)[16], which is managed by the National Cybersecurity Center (NCSC).

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.

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. The State Data Protection Inspectorate (SDI) provides detailed guidelines[17] on the use of AI systems, emphasizing the application of GDPR principles (lawfulness, data minimization, accountability). 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.

Report on the national cybersecurity exercise "Cyber Shield"[18] exercise aimed to develop practical cybersecurity skills of the exercise participants, test cyber incident management procedures, improve cooperation between institutions managing and/or investigating cyber incidents and cyber security entities, and develop public communication skills.

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

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

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

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

[18] Report on the national cybersecurity exercise "Cyber Shield OpEx 2024" (Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas OpEx 2024" ataskaita). https://www.nksc.lt/doc/KS2024_OPEX_Pratybu_ataskaita.pdf

5. National practices in selected EU Member States

2023 Open Data Best Practices in Europe. Case Study on strategies to achieve greater open data maturity in Portugal, Serbia and Slovakia. 2023.[19] This current report on open data best practices investigates the drivers behind this growth through interviews with the open data teams of these three countries. These countries were asked via a survey to share their strategies on the four dimensions of ODM: policy, impact, portal, and quality. Their insightful learnings are collected into a comprehensive overview that can serve as a learning point for other countries striving to advance their own maturity score.

The report displays the four ODM dimensions accompanied with insights from the front runner countries, making it easy for other countries to select which topic they would like to focus their improvement on. The report contributes to the goal of data sharing across countries, by making these maturity improvement options publicly available. The ODM assessment conceptualises open data maturity in four dimensions:

- Policy investigates the open data policies and strategies in place in the participating countries, the national governance models for managing open data and the measures applied to implement those policies and strategies.
- Impact analyses the willingness, preparedness and ability of countries to measure both the reuse of open data and the impact created through this reuse.
- Portal investigates the functionality of national open data portals, the extent to which users' needs and behaviours are examined in order to improve the portal, the availability of open data across different domains and the approach to ensuring the portal's sustainability.
- Quality assesses the measures adopted by portal managers to ensure the systematic harvesting of metadata, the monitoring of metadata quality and compliance with the data catalogue vocabulary application profile (DCAT-AP) metadata standard, and the quality of deployment of the published data on the national portal.

The above-mentioned countries are identified as "fastest-growing" in open data maturity. They have prioritized measuring the impact of data reuse. Therefore, the project can leverage their advancing open data portals (e.g., for threat intelligence feeds) and offer a system as a tool to measure the security "impact" of their networks.

The other example, the Nordic countries - particularly Denmark, Sweden, and Finland - are widely recognized as pioneers in digital governance and the delivery of advanced public services. Their national strategies and best practices in digitalization, which emphasize efficiency, citizen-centric design, and public-private collaboration, often serve as influential models for the broader European Union.

Danish Joint Government Digital Strategy.[20] – the strategic approach to digital initiatives makes it possible for the Danish public sector to make joint investments in areas which are particularly complex and in which there are interdependencies across different authorities, sectors, and levels of government.

Individual authorities have a responsibility to harness the digital potential within its own purview and, thus, to ensure that digital development leads to the desired change. In parallel with

[19] 2023 Open Data Best Practices in Europe. Case Study on strategies to achieve greater open data maturity in Portugal, Serbia and Slovakia. 2023. https://data.europa.eu/sites/default/files/report/2023%20Open%20Data%20Best%20Practice%20in%20Europe.pdf
[20] Danish Joint Government Digital Strategy. https://en.digst.dk/strategy/the-joint-government-digital-strategy/

joint public sector efforts, there are sector-specific digital projects and strategies, for example municipal and regional digital strategies. This approach to the digital development of the public sector provides a good balance between common strategic targets and local adaptation and priorities.

Private businesses, trade unions, and NGOs also interact with the public sector, contributing to finding common solutions for the digital transition of society and helping to secure the foundation for a strong and secure digital Denmark.

Denmark's National Strategy for Digitalisation is built upon nine core visions for the country's future. These visions encompass a wide range of policy areas, including: strengthening national cyber and information security; creating coherent digital services for citizens and businesses; using technology to improve welfare services; fostering growth in digital SMEs; building the digital healthcare of the future; accelerating the green transition through digital solutions; maintaining a strong, ethical, and responsible digital foundation; positioning Denmark at the center of international digitalization; and ensuring the entire population is ready for a digital future.

This document serves as a powerful case study of a comprehensive and forward-looking national digital strategy. Its relevance lies in its holistic approach, integrating multiple critical policy domains - security, welfare, economy, and environment - under a single, coherent digital framework. This reflects the project's overarching theme of developing integrated policy responses to complex, cross-cutting societal challenges.

Visions and recommendations for Denmark as a digital pioneer. Danish government digitization partnership[21] - This report from the Danish Government Digitisation Partnership provides a detailed set of recommendations for implementing the national strategy. Specific proposals include creating "MinVirksomhed," a digital portal to streamline interactions between businesses and public authorities. To support SMEs, it recommends establishing "robot libraries" to facilitate the adoption of automation technologies. On a European level, it calls for Denmark to take a leading role in the creation of European data spaces, particularly in areas of national strength like healthcare and climate. The report also places strong emphasis on life-long learning, proposing initiatives to embed digital skills in all levels of education and to provide personalized, digital upskilling offers for the workforce.

This source provides a practical roadmap for executing a national digital strategy. Its concrete, actionable proposals for public-private collaboration, infrastructure modernization, and workforce development offer a valuable template for how digital leadership can be achieved. It demonstrates the critical step of translating high-level vision into specific, funded initiatives.

Finland’s Cyber Security Strategy 2024–2035[22] - Finland’s Cyber Security Strategy has been revised in response to an evolving operating environment in accordance with the programme of Prime Minister Petteri Orpo’s Government. This revision accommodates the requirements imposed in the cybersecurity directive (NIS2) and other relevant key strategies and reports. The aim is to integrate the information defence entries of the Government Programme into the strategic communications model and the Government Defence Report.

Finland’s strategy emphasizes a "comprehensive security" model that relies heavily on trust-based cooperation between public authorities and the private sector, noting that businesses own

[21] Visions and recommendations for Denmark as a digital pioneer. Danish government digitization partnership. https://en.digst.dk/media/w4oft5kd/visions-and-recommendations-for-denmark-as-a-digital-pioneer-danish-government-digitisation-partnership.pdf

[22] Finland’s Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content

the majority of critical infrastructure. The document explicitly identifies that current information sharing is hindered by decentralized regulations and incompatible systems, arguing that the voluntary exchange of information must be systematized to meet the requirements of the EU NIS2 directive.

Regarding the operational capability of a monitoring system, the strategy prioritizes the development of "shared situational awareness" enabling automated monitoring and rapid response. It specifically advocates for the expansion of "centralized cybersecurity services" citing existing examples like the HAVARO threat detection system that are cost-effective and user-friendly for smaller entities like municipalities and counties. This supports the viability of the plug-in concept, provided it incorporates "security by design" principles and prepares for future technological shifts, such as the need for quantum-proof cryptography to protect data integrity by 2030.

Finally, regarding compliance and data protection, the strategy highlights the tension between intelligence gathering and privacy. It calls for updating national legislation to allow more effective sharing of threat data (including potentially personal or classified data) for attribution and criminal investigation, while strictly adhering to international law and fundamental rights. The strategy suggests that to be effective, any detection system must balance these "offensive" or intelligence-gathering capabilities with "cyber diplomacy" and strict adherence to the limitations of lawful data processing.

Sweden in a digital world. A strategy for Sweden's foreign and security policy on cyber and digital issues[23] - Sweden's strategy explicitly positions the private sector as a critical partner in national security, validating the project's aim to deploy a monitoring plug-in for governmental and private organizations.

The document emphasizes that "public-private partnerships" are essential for strengthening resilience against cross-border threats, noting that private actors own the digital infrastructure and possess the technical competence required to manage strategic technologies. The strategy calls for deepening dialogue with the business sector to establish global norms and creating confidence-building measures that facilitate information sharing between incident management authorities and private entities.

Regarding concerns about data sharing and cross-border operations, Sweden advocates for "free flows of data" balanced with "dimensioned and adapted data protection," warning against unjustified data localization requirements that hinder innovation. The strategy prioritizes regulatory interoperability between the EU, NATO, and the U.S. to prevent market fragmentation, suggesting that state of the art system should align with international standards to ensure it can operate across these jurisdictions without facing trade barriers.

[23] Sweden in a digital world. A strategy for Sweden's foreign and security policy on cyber and digital issues. https://www.government.se/contentassets/f858cec8cb944d3fa82bdf0fb7959448/sweden-in-a-digital-world---a-strategy-for-swedens-foreign-and-security-policy-on-cyber-and-digital-issues.pdf

Conclusions

The analysis of the CTI-related data sharing on cyber incidents policy practices related to GDPR requirement implementation and challenges showed that he project is highly relevant within the context of EU policy (GDPR, NIS2). However, the systems functionality must be limited: mass, indiscriminate data collection is prohibited (except for specific national security threats), biometric profiling for political purposes is banned, and decision-making transparency (explainability) must be ensured. The compliance model must rely on "Privacy by Design" and a clear distinction between civil and defense use cases.

The EU's approach to Artificial Intelligence and data protection is defined by legal acts, such as GDPR and EU AI Act, which establishes a risk-based regulatory framework to ensure AI systems are safe, transparent, and human-centric. While the Act explicitly excludes systems used for purely military purposes, it has a significant indirect influence on dual-use technologies and is expected to shape global standards. The framework promotes "Responsible AI" and "Security by Design" principles, which are complemented by NATO's own AI strategy.

This regulatory environment is further enforced by CJEU rulings such as SCHUFA Holding, which classifies algorithmic credit scores as "automated decisions" under GDPR, and Dun & Bradstreet, which affirms the "right to an explanation" for AI-driven decisions, preventing companies from hiding behind trade secrets. These legal precedents establish strict limits on indiscriminate data retention and reinforce EU privacy standards, even in national security contexts.

This information is strategically important as it demonstrates how the EU leverages its regulatory power as a tool for asserting digital sovereignty and promoting a human-centric, values-based approach to technology. The AI Act, in concert with CJEU jurisprudence, creates a distinct European model that balances innovation with fundamental rights. This framework directly interacts with national security concerns and informs transatlantic cooperation with NATO, which shares the objective of ensuring AI applications are safe and compliant with international law.

The project is highly aligned with the current geopolitical necessity for "strategic symbiosis" between the EU and NATO. The transition to a "defence-readiness mindset" creates a fertile environment for this system. There is a critical lack of automated, functioning CTI solutions for national and sectorial management.

While the strategic need is high, the legal constraints are strict. The system must navigate a narrow path between effective monitoring and illegal surveillance. The system cannot use AI for "untargeted scraping of facial images" or "biometric categorization of political opinions" (e.g., to identify foreign agents/trolls). These are "red lines".

Data Retention Limits. Under CJEU rulings (La Quadrature du Net), "mass and indiscriminate" retention of traffic data is banned for general crime fighting. The system must rely on the "quick freeze" principle, retaining data only when a specific threat arises.

Automated Decisions: If the plug-in assigns "risk scores" that automatically block traffic, it falls under GDPR Article 22. Case law (SCHUFA, Dun & Bradstreet) mandates that these decisions cannot be "black boxes"; users have a right to an explanation of the logic involved.

Recommendations

Architecture and Design (Privacy & Security). Implement "Quick Freeze" by Default: To comply with CJEU rulings for civil/commercial clients, the plug-in should not store all traffic data

indefinitely. Design it to trigger retention only upon detection of a specific anomaly or threat signature.

Pseudonymization Strategy. To facilitate information sharing between EU institutions and cross-border partners (like the projected Black Sea Hub), ensure data is transmitted in a pseudonymized format that the recipient cannot re-identify, adhering to the EDPS v SRB precedent.

"Managed Security Services" Certification. Align the project with the Union Rolling Work Programme to obtain certification as a Managed Security Service. This will provide a "presumption of conformity" with the Cyber Resilience Act (CRA) and prevent market fragmentation across Member States.

Draft a Template DPIA. Since the system will likely be classified as High-Risk (critical infrastructure/democratic processes), the project must provide clients with a template Data Protection Impact Assessment (DPIA) to lower their adoption barrier.

FIMI/Bot Detection. Calibrate the AI to detect "inauthentic behavior patterns" (bot farms) rather than profiling individuals' political views. Ensure this distinction is documented to avoid violating the AI Act's prohibition on biometric categorization.

Interoperability. Build the system to be compatible with NATO’s Data Centric Reference Architecture. The system must serve as a "single logical environment" that aggregates national, NATO, and Open Source Intelligence (OSINT) data.

References

1. Fundamentals of Secure AI Systems with Personal Data. EDPB Guidance. April 2025. https://www.edpb.europa.eu/system/files/2025-06/spe-training-on-ai-and-data-protection-technical_en.pdf
2. Guidance for Risk Management of Artificial Intelligence systems. European Data Protection Supervisor. November 2025. https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-11-11-guidance-risk-management-artificial-intelligence-systems_en
3. Apply AI Strategy (Communication from the Commission Artificial Intelligence for Europe) COM(2025) 723 final. https://eur-lex.europa.eu/resource.html?uri=cellar:194ae542-a421-11f0-97c8-01aa75ed71a1.0001.02/DOC_1&format=PDF
4. Union Rolling Work Programme for European cybersecurity certification. https://ec.europa.eu/newsroom/dae/redirection/document/102292
5. Preserving Peace - Defence Readiness Roadmap 2030. JOIN(2025) 27 final. https://defence-industry-space.ec.europa.eu/document/download/9db42c04-15c2-42e1-8364-60afb0073e68_en?filename=Joint-Communication%20_Defence-Readiness-Roadmap-2030.pdf
6. Defence Readiness Omnibus. Simplification proposal to boost industrial readiness. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-readiness-omnibus_en
7. NATO's Data Exploitation Framework Policy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/11/23/summary-of-natos-data-exploitation-framework-policy
8. Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf
9. Case C-511/18 - La Quadrature du Net and Others. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
10. Case C-634/21 - SCHUFA Holding AG. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
11. Case C-413/23 P (EDPS v SRB). Pseudonymization and AI Model Training (GDPR). September 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
12. Case C-203/22 - Dun & Bradstreet Austria GmbH. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
13. Case C-807/21 (Deutsche Wohnen). GDPR Liability and Cyber-Fines. December 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=282192&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8123480
14. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
15. National Cyber Incident Management Plan of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
16. Cybersecurity Entity Register (CISE). https://www.nksc.lt/ksis

17. The State Data Protection Inspectorate of the Republic of Lithuania. Guidelines. https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/work/
18. Report on the national cybersecurity exercise "Cyber Shield OpEx 2024" (Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas OpEx 2024" ataskaita). https://www.nksc.lt/doc/KS2024_OPEX_Pratybu_ataskaita.pdf
19. 2023 Open Data Best Practices in Europe. Case Study on strategies to achieve greater open data maturity in Portugal, Serbia and Slovakia. 2023. https://data.europa.eu/sites/default/files/report/2023%20Open%20Data%20Best%20Practice%20in%20Europe.pdf
20. Danish Joint Government Digital Strategy. https://en.digst.dk/strategy/the-joint-government-digital-strategy/
21. Visions and recommendations for Denmark as a digital pioneer. Danish government digitization partnership. https://en.digst.dk/media/w4oft5kd/visions-and-recommendations-for-denmark-as-a-digital-pioneer-danish-government-digitisation-partnership.pdf
22. Finland's Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content
23. Sweden in a digital world. A strategy for Sweden's foreign and security policy on cyber and digital issues. https://www.government.se/contentassets/f858cec8cb944d3fa82bdf0fb7959448/sweden-in-a-digital-world---a-strategy-for-swedens-foreign-and-security-policy-on-cyber-and-digital-issues.pdf

Editor
<<Main Editor>>

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

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

Disclaimer