Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

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

Project name: ***OSOTS***

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

Action result: ***Regulatory Mapping and Related Analysis***

Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Editor
Evaldas Bružė

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

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view. The users use the information at their sole risk and liability.

AI-assisted tools were used to support the drafting, structuring and linguistic refinement of this document. The final content was reviewed and approved by the authors, who remain responsible for its accuracy, integrity and suitability for use. The use of AI-assisted tools was limited to preparatory and editorial support and was not intended to infringe, misappropriate or otherwise affect any third-party proprietary, confidential, copyrighted or otherwise protected rights or materials.

Executive Summary

The OSOTS system is being developed for operational technology and industrial control system environments, including sectors where cyber incidents may affect essential services, public safety, economic activity or wider societal resilience. Although the analysis is tailored to OSOTS, its relevance is broader. The regulatory issues examined in this report are also applicable to comparable OT/ICS cybersecurity systems that monitor network activity, detect anomalies, support incident response or generate security-relevant evidence in critical or industrial environments.

The need for regulatory analysis follows from the functional character of OSOTS. The system is not a neutral technical add-on operating outside the legal environment of the infrastructure it protects. By monitoring OT/ICS networks, identifying abnormal behaviour and supporting incident analysis, OSOTS becomes part of the broader cybersecurity and resilience architecture of the deploying organisation. In such settings, cybersecurity is both a technical requirement and a legal expectation.

The value of this analysis lies in examining OSOTS as an example of a broader category of emerging cybersecurity technologies: machine-learning-enabled OT monitoring systems deployed in regulated infrastructure environments. The report therefore does not treat regulation as a separate administrative layer, but as a factor that shapes how such systems should be understood, developed and deployed.

The main regulatory focus of the report is cybersecurity and data protection. These fields are prioritised because they correspond directly to the core functions of OSOTS and similar systems. The NIS2 Directive is treated as the primary cybersecurity framework because it establishes risk-management and incident-reporting obligations for essential and important entities across the EU. Although these obligations generally apply to the deploying organisation rather than automatically to the technology itself, OSOTS is relevant because it may provide the technical basis for incident awareness, assessment and documentation.

The GDPR is treated as an equally essential framework because OT/ICS monitoring may involve personal data even where the primary purpose is technical security. Logs and other system outputs may include user identifiers, IP addresses, device identifiers, authentication records, administrator activity or other information that can be linked to identifiable individuals. The GDPR does not prevent cybersecurity monitoring, but it requires such monitoring to follow the GDPR requirements.

Other legal frameworks are considered where they help explain the wider regulatory environment of OSOTS-like systems. The Artificial Intelligence Act is relevant because OSOTS uses machine-learning-enabled anomaly detection, although the legal classification of the system depends on its intended purpose and deployment context. The Critical Entities Resilience Directive is relevant where the system contributes to the resilience of entities providing essential services. The Cybersecurity Act and Cyber Resilience Act are relevant from the perspective of product security, certification, vulnerability management and market placement. The Data Act may become relevant where the system generates or enables access to industrial data, while the Budapest Convention may be relevant where logs are used in connection with cybercrime investigation or digital evidence preservation.

The overall conclusion is that OSOTS should be analysed as a secure-by-design, privacy-by-design and audit-ready OT cybersecurity system. More broadly, the report argues that systems of this type should be assessed not only by their technical detection capacity, but also by their ability to produce reliable, interpretable and legally usable information in regulated environments. This makes OSOTS a useful case study for understanding how EU cybersecurity and data-protection law apply to emerging OT/ICS monitoring technologies.

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

Introduction

Operational technology and industrial control systems are increasingly embedded in connected, data-driven and digitally managed industrial environments. This development improves visibility, automation and operational efficiency, but it also increases exposure to cyber risks. In sectors such as energy, water, manufacturing, transport and other infrastructure-dependent domains, cyber incidents may affect not only information systems, but also physical processes, service continuity, public safety and economic resilience. This makes cybersecurity in OT/ICS environments both a technical and regulatory concern.

The OSOTS system is being developed within this broader technological and regulatory context. As an open-source operational technology sensor, OSOTS is intended to support network monitoring, anomaly detection, incident analysis and the generation of security-relevant information in industrial and critical-infrastructure environments. Although the report is tailored to OSOTS, the analysis has broader relevance for comparable OT/ICS cybersecurity systems that perform similar monitoring and detection functions in regulated operational environments.

The purpose of this report is to examine the regulatory implications of OSOTS and to identify the legal frameworks most relevant to its development, deployment and governance. The report does not treat regulation as an external layer to be considered only after technical development. Rather, it approaches regulation as part of the analytical context within which OSOTS and similar systems must be understood. This is particularly important because OT cybersecurity tools may influence incident awareness, evidence generation, data processing, operational resilience and the ability of deploying organisations to meet legal obligations.

The report adopts a selective and risk-based methodology. It is not intended to provide an exhaustive review of every legal instrument that may be indirectly connected to operational technology, cybersecurity or industrial data. Instead, it prioritises those frameworks that have the strongest normative and functional connection to OSOTS. Cybersecurity and data protection are treated as the primary areas of analysis because they correspond most directly to the system's core functions: monitoring, anomaly detection, incident analysis and the generation of security-relevant records.

For this reason, the NIS2 Directive is treated as the principal cybersecurity reference point. It is relevant because OSOTS may be deployed by organisations operating in sectors where cybersecurity risk management and incident reporting are legally significant. Similarly, the GDPR is treated as the principal data-protection framework because OT/ICS monitoring may involve the processing of data relating to identifiable natural persons, including IP addresses, metadata, access records or other technical identifiers. These frameworks are therefore prioritised not only because of their general importance in EU law, but because they correspond to the central regulatory questions raised by OSOTS.

Other legal instruments are examined as secondary frameworks where their relevance depends on the factual configuration and deployment model of the system. This includes, for example, the use of machine-learning functionality, deployment in critical-infrastructure settings, placement of the system on the EU market as hardware or software, interaction with industrial data, certification or product-security questions, and the possible evidential use of logs following cyber incidents. This approach allows the report to situate OSOTS within the wider regulatory ecosystem without overstating the direct applicability of every potentially relevant legal act.

The annexes serve a distinct but complementary analytical function. They do not replace the legal assessment in the main body of the report and do not extend the scope of applicable law. Instead, they provide supporting context through recent practices, case studies, technical observations and operational developments that help explain why the regulatory norms discussed in the main report matter in practice. The annexes are particularly relevant for understanding how cyber incidents in OT/ICS environments may affect essential services, why reliable monitoring and evidence preservation are important, and how regulatory requirements may become operationally significant in real-world deployments.

Each annex is structured as a separate contextual analysis and includes its own conclusion. These annex-specific conclusions draw out the practical relevance of the material discussed in that annex without altering the legal conclusions of the main report. In this way, the report maintains a clear distinction between

the core regulatory assessment and the broader empirical or operational material that supports it. The main body identifies and analyses the applicable legal framework, while the annexes illustrate the practical conditions under which that framework becomes relevant for OSOTS and comparable OT/ICS cybersecurity systems.

1. OSOTS System Context

OSOTS is an open-source operational technology sensor intended to improve cybersecurity in industrial and critical-infrastructure environments. It is designed to monitor OT/ICS network traffic, identify abnormal behaviour, support early detection of cyber incidents and provide security teams with the evidence needed for investigation and response. The system is particularly relevant for environments where operational continuity is critical and where conventional IT security tools may not be sufficient because industrial protocols, real-time process constraints and legacy control systems create specific risks.

The defining feature of OSOTS is that it combines passive or low-impact monitoring with machine-learning-based anomaly detection. In practical terms, this means the system observes technical events in an industrial network, builds or applies a model of expected behaviour, and identifies deviations that may indicate cyber threats, misconfiguration, unauthorised access, malware activity, lateral movement, command manipulation or other suspicious behaviour. Because OSOTS may be deployed in sensitive environments, it must be engineered so that monitoring does not disrupt the underlying industrial process.

OSOTS should be treated as a security-support system rather than as an autonomous operational-control system. Its recommended role is to detect, prioritise, explain and document anomalies, while leaving operational decisions to authorised human operators or established incident-response workflows. This distinction is legally important. A system that only supports detection and human decision-making presents a different regulatory risk profile from a system that automatically changes industrial process parameters, shuts down equipment or initiates operational containment measures without human review.

2. Methodology and Scope

The methodology of this report is regulatory, system-specific and risk-based. It does not aim to provide an exhaustive review of all legal instruments potentially connected to operational technology or cybersecurity. Instead, it focuses on the frameworks most closely linked to the OSOTS system, its intended functions and its likely deployment in OT/ICS and critical-infrastructure environments.

The main body of the report addresses applicable regulatory norms only. The analysis relies primarily on official legislative texts and authoritative institutional sources, including EU legal acts, EU institutional materials. Case-law, non-official commentary, best practices, guidelines, private-sector summaries and academic literature are not used in the main body of this report.

Cybersecurity and data protection are treated as the primary areas of analysis because they correspond directly to the core functions of OSOTS. Other legal instruments are considered as secondary frameworks where their relevance depends on the specific system configuration, deployment model, use of machine learning, market placement, interaction with industrial data or evidential use. This approach allows the report to reflect the broader regulatory environment without overstating the direct applicability of every potentially relevant legal act.

The report also distinguishes between obligations applicable to the OSOTS project and obligations applicable to deploying operators. While certain duties, such as those under NIS2, generally apply to regulated entities using the system, OSOTS must still be assessed in light of those duties because its design may determine whether operators can comply effectively. Practical recommendations and good-practice measures are addressed separately in the annexes.

3. Primary Regulatory Analysis

3.1. Cybersecurity Regulation: NIS2

The NIS2 Directive provides the principal cybersecurity framework for analysing the regulatory relevance of OSOTS in operational technology and industrial control system environments. Its relevance does not derive from OSOTS being directly classified as an essential or important entity under the Directive. Rather, it follows from the system's expected deployment context. OSOTS is intended to operate in sectors where cybersecurity incidents may affect the continuity of essential or important services, including energy, water, transport, manufacturing, public administration and other infrastructure-dependent domains. In such settings, cybersecurity monitoring is not merely a technical function, but part of the broader governance of operational resilience.

For this reason, OSOTS should be understood as a cybersecurity-enabling component within the risk-management framework of the deploying organisation. The NIS2 Directive places the primary legal obligations on entities falling within its sectoral and organisational scope, while technology suppliers and tools are relevant insofar as they shape the ability of those entities to manage risks effectively. OSOTS is therefore legally relevant because it may contribute to the detection, interpretation and documentation of cyber events in regulated environments.

This is particularly significant in OT/ICS contexts. Industrial systems differ from ordinary IT environments because the priority is not only confidentiality and integrity, but also continuity, safety and availability. A monitoring system deployed in this context must therefore be assessed by reference to its capacity to support situational awareness without disturbing the industrial process itself. From a NIS2 perspective, the value of OSOTS lies in its ability to contribute to risk visibility, incident understanding and resilience in environments where delayed or unclear detection may have consequences beyond the digital layer.

The reporting structure under NIS2 further explains why OSOTS-generated information is legally important. The Directive requires staged reporting of significant incidents, beginning with early warning and followed by more detailed notification and final reporting. This does not mean that OSOTS should determine whether a legal notification is required. That assessment remains with the deploying organisation. However, the system may provide the factual basis on which that assessment depends. Its outputs must therefore be capable of supporting a reasoned understanding of the incident, including the nature of the anomaly, affected systems, potential operational impact and possible wider implications.

NIS2 also places emphasis on accountability and evidence in cybersecurity governance. In practice, a cyber incident may require internal escalation, management review, communication with cybersecurity authorities, or later audit. OSOTS is relevant to each of these processes because it may produce the technical record from which the incident is reconstructed. The integrity, traceability and interpretability of logs and alerts are therefore not only technical qualities; they are conditions for the regulatory usefulness of the system.

The open-source character of OSOTS adds a further dimension to the NIS2 analysis. Open-source development may support transparency, adaptability and independent scrutiny. At the same time, it raises questions concerning dependency management, software updates, external contributions and the security of the development pipeline. Since NIS2 gives particular attention to supply-chain security and the quality of products and service providers, the governance of OSOTS as an open-source security tool is part of its regulatory assessment.

Overall, NIS2 is relevant to OSOTS because it provides the legal framework within which cybersecurity monitoring, incident evidence, supply-chain reliability and operational resilience must be evaluated. OSOTS is not merely a sensor in technical terms. In NIS2-regulated environments, it may become part of the institutional capacity to understand, manage and document cybersecurity risk. Its regulatory significance therefore depends on whether it can provide reliable security insight while respecting the operational constraints of OT/ICS environments.

3.2. GDPR and Data Protection Requirements

The GDPR is central to the regulatory assessment of OSOTS because cybersecurity monitoring in OT/ICS environments may involve the processing of data relating to identifiable individuals. Although OSOTS is primarily designed to analyse technical and operational network activity, its outputs may include usernames, administrator identifiers, workstation identifiers, IP addresses, device identifiers, access records, remote-access logs or other data capable of being linked to operators, engineers, contractors or system administrators. In this context, the distinction between "technical data" and "personal data" is not absolute: where technical records allow a natural person to be identified directly or indirectly, they fall within the scope of the GDPR.

The relevance of the GDPR does not mean that cybersecurity monitoring is legally problematic in itself. On the contrary, the protection of networks, information systems and operational continuity may provide a legitimate and necessary basis for processing. The legal issue is therefore not whether OSOTS may support security monitoring, but under what conditions such monitoring remains lawful, proportionate and compatible with data-protection principles.[2] In the OSOTS context, this requires particular attention to purpose limitation, data minimisation, storage limitation, integrity, confidentiality and accountability.[3]

The purpose of OSOTS processing is especially important. A system developed for OT cybersecurity should be legally and functionally distinguished from systems used for employee surveillance, productivity monitoring or behavioural evaluation. The same log data may have different legal significance depending on the purpose for which it is used. Processing that is proportionate for incident detection, forensic analysis or system-integrity monitoring may become more intrusive if reused for unrelated employment, disciplinary or behavioural-profiling purposes. This makes purpose definition a central element of the GDPR analysis rather than a purely administrative matter.

The applicable lawful basis depends on the deployment model and the role of the actor operating the system. In private-sector contexts, network and information security may in some cases be assessed under legitimate interests. In public-sector or regulated critical-infrastructure contexts, processing may instead be linked to a legal obligation or to the performance of a task carried out in the public interest. The GDPR assessment must therefore remain contextual: OSOTS does not have a single universal lawful basis, because the legal character of the processing depends on who deploys the system, for what purpose, and under which legal mandate.

Data protection by design and by default is particularly relevant for OSOTS because the system's privacy impact is shaped by architectural choices made before deployment. In OT/ICS monitoring, these choices include the level of network visibility, the granularity of logs, the treatment of identifiers, the separation of raw technical data from aggregated alerts, and the default retention of security records. The GDPR therefore requires the privacy impact of OSOTS to be assessed as part of the system's design logic, not merely as a later compliance layer.

Pseudonymisation is significant but should not be overstated. Replacing usernames, IP addresses or device identifiers with pseudonymous values can reduce exposure of individuals during routine analysis. However, pseudonymised data remains personal data where re-identification remains possible. In OSOTS deployments, this is likely to be the case where the deploying organisation retains the means to link pseudonymous values back to specific users or devices. Pseudonymisation therefore operates as a risk-reduction measure, not as a way of removing the system from the GDPR framework.

Retention is another legally significant issue. Cybersecurity monitoring may require logs to be retained long enough to detect patterns, reconstruct incidents and support post-incident analysis. At the same time, indefinite retention of identifiable technical records is difficult to reconcile with the principle of storage limitation. For OSOTS, the regulatory question is therefore how long different categories of data remain necessary for the defined security purpose. Raw technical records, alerts, aggregated indicators and confirmed incident evidence may each justify different retention periods, depending on their evidential and operational value.

The security of OSOTS data is itself a data-protection issue. A compromise of OSOTS logs could expose network structure, access patterns, administrative activity, vulnerabilities or incident evidence. This means

that the system is not only a tool for protecting other systems; it also becomes a repository of sensitive security-relevant information. The GDPR therefore makes the confidentiality, integrity and availability of OSOTS data part of the legal assessment of the system.

Personal data breach rules are relevant where OSOTS data contains information linked to identifiable individuals. If logs or incident records are accessed, altered, lost or disclosed without authorisation, this may amount to a personal data breach. The legal significance of such an event depends on the risk posed to the rights and freedoms of individuals, but the possibility of breach notification must be considered in the overall assessment of OSOTS deployments.

Finally, large-scale or sensitive OSOTS deployments may require a Data Protection Impact Assessment. This is particularly relevant, for example, where monitoring is centralised across several sites, where access records are correlated over time, where the system processes data relating to employees or contractors, or where machine-learning components are used to infer behavioural patterns. In such cases, the GDPR assessment must consider not only data security, but also broader risks to individuals, including excessive monitoring, misinterpretation of behaviour, unjustified access to identifiable records and lack of effective control over secondary use.

Overall, the GDPR is relevant to OSOTS because OT cybersecurity monitoring can generate legally significant personal data even where the system's primary purpose is technical security. The regulatory assessment therefore depends on whether OSOTS can support cybersecurity objectives while preserving the core data-protection requirements of legality, proportionality, purpose limitation, data minimisation, security and accountability. In this sense, GDPR compliance is not external to the cybersecurity function of OSOTS; it is part of the conditions under which that function can be lawfully and responsibly performed.

4. Secondary Regulatory Frameworks

4.1. AI Act

The AI Act is relevant because OSOTS includes machine-learning-based anomaly detection. The key legal question is whether the OSOTS AI component qualifies as a high-risk AI system in a particular deployment. The European Commission explains that high-risk classification depends on the intended purpose of the AI system and the function it performs.

OSOTS should therefore be assessed in two layers. The first layer is whether it is an AI system under the AI Act. A machine-learning anomaly-detection component that generates predictions, risk scores or classifications based on network data is likely to fall within the broad AI concept. The second layer is whether it is high-risk. The Commission explains that AI systems can be high-risk if embedded as safety components in products covered by relevant product legislation or if intended for high-risk use cases listed in Annex III. Annex III includes AI systems used as safety components in certain critical infrastructures, including road traffic and the supply of water, gas, heating and electricity.

OSOTS should not be described categorically as high-risk in every deployment. If it only provides advisory alerts to a human SOC analyst and does not automatically control industrial operations, it may not always meet the threshold. However, if OSOTS is integrated into operational response workflows that automatically isolate network segments, block commands, trigger shutdown procedures or materially affect the management of critical infrastructure, high-risk analysis becomes much stronger.

Even where OSOTS is not legally high-risk, the project should adopt several AI Act-aligned controls because they are good practice for OT safety and trust. These include model documentation, dataset governance, performance testing, false-positive and false-negative monitoring, human oversight, cybersecurity protection of the ML pipeline, logging of model outputs, and clear instructions for use. For high-risk AI systems, the Commission identifies obligations such as risk management, data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity and robustness. These obligations are also sensible design principles for OSOTS even where the classification remains uncertain.

The OSOTS user interface should explain why an anomaly was flagged. A useful explanation might identify the baseline behaviour, the deviation, affected assets, confidence score, relevant historical context and recommended human review steps. The explanation should be written for OT security teams, not only

data scientists. In critical infrastructure, explainability is necessary because operators must understand whether an alert reflects a cyberattack, a process change, a maintenance event, a sensor error or a benign operational deviation.

4.2. Critical Entities Resilience Directive

The Critical Entities Resilience Directive is secondary but important in deployments involving essential services. The Directive aims to strengthen the resilience of critical entities against threats such as natural hazards, terrorist attacks, insider threats, sabotage and public-health emergencies. It also requires Member States to adopt national strategies, carry out risk assessments and identify critical entities.

OSOTS can support CER compliance indirectly by improving the operator's visibility over cyber and cyber-physical risks. It can help identify anomalies that may threaten service continuity, provide evidence for risk assessments, and support incident-response and business-continuity planning. However, CER is broader than cybersecurity. It covers resilience against multiple hazards, so OSOTS should be positioned as one component of a wider resilience programme rather than as a complete CER compliance solution.

For CER purposes, OSOTS should provide resilience-relevant outputs: affected service, affected site, potential operational impact, dependency mapping, duration of anomaly, and evidence of restoration. These outputs can support continuity exercises, post-incident reviews and resilience planning.

4.3. Cybersecurity Act and EU Cybersecurity Certification

The EU Cybersecurity Act established the EU cybersecurity certification framework. The European Commission explains that the framework provides EU-wide certification schemes based on technical requirements, standards and procedures, and that certificates are recognised across EU Member States. Certification schemes can use assurance levels such as basic, substantial and high, depending on the risk associated with the intended use of the product, service or process.

For OSOTS, certification should be treated as a trust and market-readiness issue. It may not be mandatory in all cases, but it will be commercially and operationally important for deployment in critical sectors. The Commission notes that the first EU Cybersecurity Certification Scheme on Common Criteria applies on a voluntary basis and includes categories such as firewalls, detection and response platforms, routers, switches, specialised software including SIEM and IDS/IDP systems, and data diodes. OSOTS is closely aligned with the detection and response / IDS category, so certification readiness should be built into the project.

Certification readiness requires secure development documentation, architecture diagrams, threat models, vulnerability-management procedures, test results, dependency control, release management, access-control evidence, cryptographic design documentation and audit logs. These materials should not be created only at the end of development. They should be maintained continuously as part of engineering governance.

4.4. Cyber Resilience Act

The Cyber Resilience Act is likely to become highly relevant if OSOTS is supplied on the EU market as software, hardware, a sensor appliance, a managed product or a component with digital elements. The Commission explains that the CRA applies to hardware and software products with digital elements made available on the EU market and aims to set conditions for secure hardware and software development.

The CRA requires manufacturers to meet essential cybersecurity requirements during design, development, production and maintenance. It also introduces lifecycle vulnerability handling and, for some products, third-party assessment. The main CRA obligations apply from 11 December 2027, while reporting obligations apply from 11 September 2026.

For OSOTS, the CRA creates practical requirements even before full application. The project should maintain a cybersecurity risk assessment, technical documentation, vulnerability-handling process, secure-by-default configuration, update mechanism, support-period policy and user instructions for secure installation and operation. The Commission's summary states that manufacturers must notify actively

exploited vulnerabilities and severe incidents affecting product security, with deadlines including 24 hours for early warning and 72 hours for the main notification.

Because OSOTS is open source, the project should carefully assess whether it is merely published as free and open-source software or made available on the market in the course of a commercial activity. The CRA contains a specific concept of an open-source software steward, described as a legal person that systematically provides sustained support for specific free and open-source software intended for commercial activities and ensures its viability. This distinction may be important for OSOTS governance.

4.5. Data Act

The Data Act is relevant because OSOTS may generate industrial operational data, alerts, derived metrics and telemetry. The European Commission explains that the Data Act aims to make data, particularly industrial data, more accessible and usable, and gives users of connected products greater control over data they generate. It applies from 12 September 2025.

For OSOTS, the Data Act does not replace GDPR or cybersecurity law. It sits alongside them. Operators should be able to access and export OSOTS-generated data in structured and usable formats, but sharing must not undermine cybersecurity, confidentiality or data protection. If OSOTS data includes personal data, GDPR continues to apply. If OSOTS data includes sensitive security data, access controls and contractual restrictions may be necessary to avoid creating new cybersecurity risks.

The system should therefore provide documented export formats, APIs and access logs. It should distinguish between raw security data, alerts, aggregated metrics, model outputs and customer-specific configurations. External data sharing should be controlled by the deploying organisation and logged.

4.6. Budapest Convention on Cybercrime

The Budapest Convention is relevant where OSOTS logs may support cybercrime investigation or international cooperation. The Convention includes provisions on international cooperation, mutual assistance and expedited preservation of stored computer data. Official Council of Europe materials identify Article 29 as dealing with expedited preservation of stored computer data.

OSOTS is not a law-enforcement system, but it may generate evidence that later becomes relevant to investigations. Therefore, OSOTS logs should be integrity-protected, timestamped, exportable and accompanied by chain-of-custody information. The system should record who accessed logs, who exported them, when they were exported, what filters were applied and whether the exported package was cryptographically hashed. These features support evidential reliability and reduce disputes about authenticity.

5. OSOTS Compliance-by-Design Requirements

OSOTS should be developed around a compliance-by-design model that integrates cybersecurity, GDPR, AI governance and product-security requirements into the system lifecycle. The model should be practical enough for engineers and auditors to use, but sufficiently structured to support legal accountability.

The first requirement is clear role allocation. Deployment documentation should identify whether OSOTS operates fully on-premises, whether any telemetry is transmitted to the OSOTS project, whether remote support has access to logs, whether data is used for model improvement, and whether third-party infrastructure is involved. This determines GDPR roles, contractual requirements and transfer risks.

The second requirement is secure architecture. OSOTS should use passive or low-impact monitoring by default, separate sensor, management and analytics functions, protect communications through encryption, authenticate all administrative access, and maintain tamper-evident logs. The system should not create new pathways from IT networks into OT environments. Remote administration should be disabled by default or subject to strict controls.

The third requirement is data minimisation. OSOTS should collect the least intrusive data that still supports detection, response and forensic needs. Metadata and protocol-level features should be preferred

over full content capture. Where raw capture is required, it should be exceptional, justified, access-restricted and subject to short retention.

The fourth requirement is incident-reporting readiness. OSOTS should help operators meet NIS2 timelines by producing early-warning evidence within minutes, not hours. The system should include incident packages that can be exported for internal management, SOC review, CSIRT communication and legal assessment. These packages should include technical facts without unnecessary personal or commercially sensitive data.

The fifth requirement is GDPR operational control. OSOTS should include configurable retention, pseudonymisation, access control, audit logging, export approval, breach-detection for its own data repositories and DPIA-support documentation. It should also provide a clear data inventory and records of processing support for customers.

The sixth requirement is ML governance. OSOTS should document model purpose, input data, output meaning, confidence scoring, limitations, known failure modes, update process and validation results. Models should be tested for false positives and false negatives in representative OT environments. Operators should be able to understand whether an alert is based on a known signature, statistical deviation, learned pattern or correlation across events.

The seventh requirement is vulnerability and update governance. OSOTS should maintain a coordinated vulnerability disclosure policy, software bill of materials, dependency tracking, signed releases, secure update channels and support-period policy. Vulnerabilities affecting OSOTS itself must be handled with urgency because compromise of the sensor could expose sensitive security information.

The eighth requirement is audit readiness. OSOTS should generate evidence that can withstand internal audit, regulatory review and post-incident investigation. Audit logs should be protected from alteration, retained according to policy, and exportable in a format that preserves integrity and context.

6. Summary and Conclusion

OSOTS is best understood as a cybersecurity and compliance-support system for OT and ICS environments. Its main regulatory function is to help organisations detect cyber incidents earlier, understand them more clearly, preserve reliable technical evidence, and meet their cybersecurity and data-protection obligations in a controlled and accountable way. The legal analysis confirms that cybersecurity and GDPR requirements must remain the centre of the OSOTS compliance strategy. NIS2 is the primary cybersecurity framework because OSOTS is intended for sectors and environments where continuity, resilience and incident response are legally significant. The system should therefore support risk management, monitoring, incident handling, reporting, supply-chain security, vulnerability management and audit readiness. In particular, OSOTS should be capable of producing structured information that helps operators meet the NIS2 reporting sequence of 24-hour early warning, 72-hour incident notification and final reporting within one month.

GDPR is equally important because OT cybersecurity monitoring may involve personal data, even where the main purpose of the system is technical security. OSOTS logs may contain usernames, IP addresses, device identifiers, access events or administrator actions. These data points may identify individuals directly or indirectly. For that reason, OSOTS must implement privacy-preserving defaults, including data minimisation, pseudonymisation, role-based access control, configurable retention, secure logging, encryption, export controls and clear separation between security monitoring and any unrelated employee-monitoring purposes.

The AI Act, CER Directive, Cybersecurity Act, Cyber Resilience Act, Data Act and Budapest Convention supplement this core analysis. They do not replace the NIS2 and GDPR focus, but they shape the broader compliance environment. The AI Act requires careful assessment of the machine-learning component, particularly where OSOTS is used in critical infrastructure or as part of operational decision-making. The CER Directive reinforces the importance of resilience and continuity. The Cybersecurity Act supports certification readiness and assurance. The Cyber Resilience Act strengthens the need for secure development, vulnerability handling and lifecycle security if OSOTS is placed on the EU market as a product

with digital elements. The Data Act may affect access to industrial data generated by OSOTS. The Budapest Convention is relevant where system logs may be used as digital evidence.

The final compliance position is therefore clear. OSOTS should not be designed as a simple monitoring add-on. It should be designed as a regulated security component for high-consequence environments. This requires secure architecture, privacy-conscious data handling, explainable machine-learning outputs, human oversight, strong audit trails, vulnerability management, incident-reporting support and documentation that allows operators to demonstrate compliance. If these requirements are built into the system from the outset, OSOTS can support both operational security and legal accountability in critical OT environments.

Bibliography

- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities, available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification, available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data, available at https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
- Council of Europe Convention on Cybercrime, Budapest, 23 November 2001, available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
- Lietuvos Respublikos kibernetinio saugumo įstatymas / Republic of Lithuania Law on Cyber Security. Consolidated Lithuanian version: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr
- European Commission – NIS2 Directive policy page, available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- European Commission – NIS2 questions and answers, available at: https://digital-strategy.ec.europa.eu/en/revision-network-and-information-security-directive-questions-and-answers
- European Commission – AI Act official guidance / navigation page, available at: https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act
- European Commission – Cyber Resilience Act policy page, available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- European Commission – Cyber Resilience Act implementation FAQ, available at: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions
- European Commission – EU Cybersecurity Certification Framework, available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
- European Commission – Data Act explained, available at: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

- European Commission – Critical infrastructure resilience at EU level, available at: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

ANNEX 1
RECENT PRACTICES

This document reviews recent policy practices primarily on the level of EU and NATO institutions highlighting potential product compliance with GDPR, AI Act and cybersecurity practices. It also covers relevant policy practices in Lithuania and several other EU Member States.

1. Scope of sources

1.1. Strategic and policy documents (EU/NATO)

1. The Union Rolling Work Programme for European cybersecurity certification[1]

For projects like this, building security and privacy into the foundation is a non-negotiable requirement. According to the Union Rolling Work Programme, security isn't something you "add on" later. It must be integrated from the very first design phase. This involves practicing "data minimization," which means only gathering the bare essentials needed to spot a threat (for instance, looking at data headers instead of scaning through full packet contents).

Relevance:

- Strategic Alignment. The document highlights a major shift in European cybersecurity, showing how voluntary certification and the mandatory rules of the Cyber Resilience Act (CRA) work together.
- For this project, earning a European cybersecurity certificate serves as proof that the product meets the CRA's strict legal standards. This gives a strong reason to adopt "security-by-design" and "security-by-default" habits, ensuring handlingvulnerabilities carefully throughout the software's entire lifespan.
- Future-Proofing Services. Managed Security Services (MSS), such as incident response and security audits, are set to be the next big focus for EU certification. Because this project is building a "cyber threat management system," these upcoming rules apply directly. Getting certified under this new framework would allow the service to operate smoothly across all EU member states without having to comply with different sets of national laws.
- Faster Certification for Modern Software. Traditional certification can be too slow for software that updates constantly. To solve this, the document suggests "fixed-time evaluation" methods, which are specifically designed to be flexible and cost-effective for SMEs. It also encourages following a "Secure Development Lifecycle" (SDL) and adopting industry standards (like ISO/IEC 27034) early on, making the eventual path to compliance much smoother.

2. European Defence Industrial Strategy (EDIS) (March 2024)[2]

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**.

Relevance:

- 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 EU and NATO.
- The strategy proposes the creation of a European Defence Industry Group and an "Innovation Office" to bridge the gap between startups and military needs, thereby fostering a "trust dividend" for EU-made solutions.
- 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.

3. White paper on options for enhancing support for research and development involving technologies with dual-use potential.[3]

The European Commission White Paper on options to enhance support for research and development involving technologies with dual-use potential addresses the separation between civilian and defense R&D, proposing options to bridge this gap particularly for critical technologies like Artificial Intelligence (AI) and cybersecurity tools.

Relevance:

- The document defines dual-use consistent with Regulation (EU) 2021/821, focusing on software and technologies that serve both civilian and military strategic objectives.
- It encourages synergies that allow civilian-driven innovations to strengthen the defense industrial base and accelerate the market uptake of high-stakes services.
- The document 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.

4. Defense and artificial intelligence. European Parliament Briefing (April 2025).[4]

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.

Relevance:

- 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).

- The document 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.

5. "Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies (EDTs)" (February 2021)[5]

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.

Relevance:

- The document emphasizes 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.
- 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.

6. Data Strategy for the Alliance (May 2025)[6]

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.

Relevance:

- 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.

7. European Commission. European approach to artificial intelligence, policy review (2025)[7].

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.

Relevance:

- The document focuses on commercial and public sector AI, it underscores that building high-performance, and robust systems requires high-quality data, which is supported by broader initiatives like the EU Cybersecurity Strategy and the Data Union Strategy.
- Commission 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.

8. AI Continent Action Plan (April 2025)[8]

The the "AI Continent Action Plan" focuses on the implementation of the EU AI Act to create a single market for trustworthy and human-centric AI.

Relevance:

- Establishing support structures like the AI Office and an AI Act Service Desk are important initiatives in order to assist with regulatory compliance.
- Among other, the document confirms that the AI Act will function alongside existing legislation such as the GDPR and emphasizes strict safeguards for data security, confidentiality, and integrity within the Data Union Strategy.
- 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.

9. Apply AI Strategy (October 2025)[9]

The Commission Communication COM(2025) 723 "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**, defense, security, and space.

Relevance:

- 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 discussion 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.
- 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.
- 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.

10. Action Plan on Synergies between Civil, Defence and Space Industries (Feb 2021)[10]

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. It identifies Artificial Intelligence (AI), cybersecurity, and data cloud infrastructures as "critical technologies" where synergies between civil and defense domains offer substantial potential while ensuring mandatory compliance with European data protection (GDPR) and ethical standards.

Relevance:

- 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 monitordependencies 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.

11. Defence Readiness Omnibus. Simplification proposal to boost industrial readiness[11]

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 defenceinvestments over the next four years, enabling Member States and industry to respond swiftly and effectively to growing threats.

Relevance:

- 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.
- The "Defence Readiness Omnibus" represents a major regulatory shift aimed at mobilizing up to €800 billion in investments and establishing a "defence-readiness mindset" that creates a more favorable environment for particular projects.
- This package is directly relevant to developing a cyber threat management system as it explicitly prioritizes the acceleration of next-generation technologies in the cyber domain, alongside land, air, sea, and space. It introduces significant simplifications to the European Defence Fund (EDF), ensuring faster time-to-grant and reduced administrative burdens, which is particularly beneficial since 43% of current EDF participants are SMEs.

12. Digital Omnibus proposal[12]

The Digital Omnibus proposal includes a set of technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, and to stimulate competitiveness. It is a first step to optimisethe application of the digital rulebook. The immediate objective is to ensure that compliance with the rules comes at a lower cost, delivers on the same objectives, and brings in itself a competitive advantage to responsible businesses.

Relevance:

- The Digital Omnibus Regulation might be relevant for the project, as it aims to streamline the complex regulatory environment the project is navigating.
- The proposal introduces a set of technical amendments across a wide corpus of digital legislation, specifically covering cybersecurity, artificial intelligence, data policy, and privacy with the explicit goal of "optimizing the application of the digital rulebook".
- This proposal is designed to shift the focus from heavy administrative burdens to growth, allowing businesses from start-ups to established enterprises to spend less time on paperwork and more time "innovating and scaling-up".
- This suggests that the future compliance landscape for cyber threat management system may become less fragmented and resource-intensive than current GDPR and AI Act provisions imply.

13. The Helsinki Statement on enhanced clarity, support and engagement (July 2025)[13]

The European Data Protection Board has adopted the Helsinki statement. The members of EDPB agreed on new initiatives to facilitate easier GDPR compliance, to enhance the dialogue with a broad range of stakeholders, to strengthen consistency and to develop cross-regulatory cooperation in the new digital regulatory landscape.

Relevance:

- These initiatives enable, in particular, micro, small and medium organisations; empower responsible innovation; and reinforce competitiveness in Europe.
- The EDPB members underlined the essential role of data protection in upholding European values and individuals' fundamental rights, and supporting the human-centric use of personal data.
- Across its efforts, the EDPB will strengthen its dialogue with stakeholders, holding proactive and early engagement to identifyspecific areas where further support and clarification is required, and providing the opportunity for stakeholders to flag possible inconsistencies and give feedback.
- The EDPB will publicly report on the main outcomes of public consultations.
- The EDPB notes the importance of also providing timely and concise guidance that is accessible, easy to understand, and practical for micro, small and medium organisations in line with the risk-based approach. With this in mind, the EDPB agreed to update its working methods and to develop complementary formats for guidance.

1.2. Recommendations, guidelines, codes of practice

1. Commission Guidelines on Prohibited AI Practices (Feb 2025)[14]

Commission Guidelines set the barriers for the project, specifically outlining what AI systems are strictly forbidden. If the sensortracks how data is collected, it must be ensured it doesn't use any AI methods labeled as "unacceptable risk." These guidelines were created to make sure the EU AI Act is applied the same way

across all member states. The document provides clear explanations and real-world examples to help the project stay compliant.

Relevance:

- 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.

2. EDPB Guidance "Fundamentals of Secure AI Systems with Personal Data" (April 2025)[15]

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 source outlines a training curriculum for cybersecurity professionals working with personal data and artificial intelligence (AI) in the European Union (EU).

***Relevance*:**

- 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.
- 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.

3. Guidance for Risk Management of Artificial Intelligence systems. European Data Protection Supervisor (November 2025)[16]

The Guidance defines risk-based approach. This Guidance aims to guide EUIs acting as data controllers in identifying and mitigating some of these risks by employing such strategies as fairness, accuracy, data minimization, security and data subjects' rights. EDPS guidance indicates that data controllers must conduct a Data Protection Impact Assessment (DPIA), especially when using AI.

Relevance:

- 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 cyber attacks, often orchestrated by state-aligned groups to destabilize EU society, including critical infrastructure, energy sector, etc.

4. Guidelines 01/2025 on Pseudonymisation (January 2025)[17]

The GDPR defines the term 'pseudonymisation' for the first time in EU law and refers to it several times as a safeguard that may be appropriate and effective for the fulfilment of certain data protection obligations.

Relevance:

- These guidelines take a closer look at the legal definition of pseudonymisation and the terms used therein. What is attribution? What is to be considered additional information? A key aspect evolving from this analysis are the many options for controllers to tailor their pseudonymisation processes to the objectives they intend to achieve.
- The guidelines introduce a new concept, called pseudonymisation domain, to capture one aspect of that freedom: to determine who should be precluded from attributing the pseudonymised data to individuals.
- The guidelines show how controllers and processors can use pseudonymisation to meet data-protection requirements. While pseudonymisation is a powerful and relevant measure, the document shows that it will always need to be complemented by further measures. The Guidelines highlight the benefits of pseudonymisation. They show in particular how pseudonymisation serves as a measure for data protection by design and by default, and as a measure contributing to ensuring a level of security appropriate tothe risk of processing. At least in the latter case, the effect of pseudonymisation will have to be measured against the capabilities of persons or parties acting without authorisation.
- The guidelines look at the implementation of pseudonymisation. How should personal data be transformed to pseudonymise it? How should unauthorised attribution be prevented? How should different pseudonymised data sets be linked, and how could such linkage be controlled?

5. Guidelines 3/2025 on the interplay between the DSA and the GDPR (September, 2025)[18]

These guidelines aim to contribute to the consistent interpretation and application of the DSA and of the GDPR insofar as some provisions of the DSA concern the processing of personal data by intermediary service providers and include references to GDPR concepts and definitions. The guidelines focus on specific provisions of the DSA where there is a significant interplay with the GDPR.

Relevance:

- Article 25(2) DSA provides that the prohibition of Article 25(1) DSA for providers of online platforms to deploy deceptive design patterns in their interfaces shall not apply to practices of those providers that are covered by the GDPR. The guidelines mention key elements to consider when assessing whether a deceptive design pattern is covered by the GDPR, in particular whetherpersonal data is being processed and whether the data subject's behaviour that the pattern is influencing relates to the processing of personal data. Such key elements are complemented by examples of cases where deceptive design patterns are or are not covered by the GDPR.

6. Orientations on generative Artificial Intelligence (generative AI) and personal data protection (September 2025)[19]

EDPS Orientations on generative Artificial Intelligence (generative AI) and personal data protection intend to provide practical advice and instructions to EU institutions, bodies, offices and agencies (EUIs) on the processing of personal data when using generative AI systems, to facilitate their compliance with their data protection obligations as set out, in particular, in Regulation (EU) 2018/1725. These orientations have been drafted to cover as many scenarios and applications as possible and do not prescribe specific technical measures. Instead, they put an emphasis on the general principles of data protection that should help EUIs comply with the data protection requirements according to Regulation (EU) 2018/1725.

Relevance:

Revised orientations offer more detailed guidance taking into account the evolution of Generative AI systems and technologies, their use by EUIs, and the results of the EDPS' monitoring and oversight activities.

- These orientations do not aim to cover in full detail all the relevant questions related to the processing of personal data in the use of generative AI systems that are subject to analysis by data protection authorities. Some of these questions are still open, and additional ones are likely to arise as the use of these systems increases and the technology evolves in a way that allows a better understanding on how generative AI works.
- Because artificial intelligence technology evolves quickly, the specific tools and means used to provide these types of services are diverse and they may change very quickly. Therefore, these orientations have been drafted to cover as many scenarios and applications as possible.
- The first orientations, issued in 2024, served as a preliminary step towards the development of more comprehensive guidance by the EDPS. In 2025, these orientations have been revisited and expanded, providing further clarification and additional elements to support EUIs in the development and implementation of these systems. The guidance may continue to be updated, refined, and expanded over time to address emerging needs and ensure effective implementation.

7. Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (October 2024)[20]

These guidelines analyse the criteria set down in Article 6(1)(f) GDPR that controllers must meet to lawfully engage in the processing of personal data that is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party".

Relevance:

- In order to determine whether a given processing of personal data may be based on Article 6(1)(f) GDPR, controllers should carefully assess and document whether these three cumulative conditions are met. This assessment should be done before carrying out the relevant processing operations.
- With regard to the condition relating to the pursuit of a legitimate interest, not all interests of the controller or a third party may be deemed legitimate; only those interests that are lawful, precisely articulated and present may be validly invoked to rely on Article 6(1)(f) GDPR as a legal basis. It is also the responsibility of the controller to inform the data subject of the legitimate interests pursued where that processing is based on Article 6(1)(f) GDPR.
- With regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, it should be ascertained whether the legitimate interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, also taking into account the principles enshrined in Article 5(1) GDPR. If such other means exist, the processing may not be based on Article 6(1)(f) GDPR.
- With regard to the condition that the interests or fundamental rights and freedoms of the person concerned by the data processing do not take precedence over the legitimate interests of the controller or of a third party, that condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the relevant processing. The processing may take place only if the outcome of this balancing exercise is that the legitimate interests being pursued are not overridden by the data subjects' interests, rights and freedoms.
- A proper Article 6(1)(f) GDPR assessment is not a straightforward exercise. Rather, the assessment requires full consideration of a number of factors, such as the nature and source of the relevant legitimate interest(s), the impact of the processing on the data subject and their reasonable expectations about the processing, and the existence of additional safeguards which could limit undue impact on the data subject.

- The guidelines provide guidance on how such an assessment should be carried out in practice, including in a number of specific contexts (e.g., fraud prevention, direct marketing, information security, etc.) where this legal basis may be considered.

8. The General-Purpose AI Code of Practice[21]

The Code of Practice helps industry comply with the AI Act legal obligations on safety, transparency and copyright of general-purpose AI models. The General-Purpose AI (GPAI) Code of Practice is a voluntary tool, prepared by independent experts in a multi-stakeholder process, designed to help industry comply with the AI Act's obligations for providers of general-purpose AI models.

Relevance:

- The code, consisting of three separately authored chapters: Transparency, Copyright, and Safety and Security. helps industry comply with the AI Act legal obligations on safety, transparency and copyright of general-purpose AI models.
- The Chapters on Transparency and Copyright offer all providers of general-purpose AI models a way to demonstrate compliance with their obligations under Article 53 AI Act.
- The Chapters on Safety and Security is only relevant to the small number of providers of the most advanced models, those that are subject to the AI Act's obligations for providers of general-purpose AI models with systemic risk under Article 55 AI Act.

9. First Draft Code of Practice on Transparency of AI-Generated Content[22]

This first draft of the Code addresses key considerations for providers and deployers of AI systems generating content falling within the scope of Article 50(2) and (4).

Relevance:

- Code aims to ensure that AI-generated and manipulated content are marked in a machine-readable and detectable manner with technical solutions that are effective, reliable, robust and interoperable.
- It seeks to make it easier for natural persons to identify deepfakes and AI-generated or manipulated text which is published with the purpose of informing the public on matters of public interest.

10. Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)[23]

The AI Act does not apply to all systems, but only to those systems that fulfil the definition of an 'AI system' within the meaning of Article 3(1) AI Act. The definition of an AI system is therefore key to understanding the scope of application of the AI Act.

Relevance:

- By issuing these Guidelines, the Commission aims to assist providers and other relevant persons, including market and institutional stakeholders, in determining whether a system constitutes an AI system within the meaning of the AI Act, thereby facilitating the effective application and enforcement of that Act.
- Considering the wide variety of AI systems, it is not possible to provide an exhaustive list of all potential AI systems in these Guidelines. This is in line with recital 12 AI Act, which clarifies that the

notion of an 'AI system' should be clearly defined while providing 'the flexibility to accommodate the rapid technological developments in this field'. The definition of an AI system should not be applied mechanically; each system must be assessed based on its specific characteristics.

11. Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation[24]

The Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR) pursue different purposes and objectives and have different scopes. While the GDPR aims to protect natural persons with regard to the processing of personal data and ensure the free flow of personal data in the Union covering all data controllers and processors, the DMA aims to tackle unfair practices, and their potential harmful effects for business users, by laying down harmonised rules applicable to gatekeepers ensuring, for all businesses, contestable and fair markets in the digital sector across the Union, to the benefit of both business users and end users.

Relevance:

- Article 5(2) DMA prohibits gatekeepers from carrying out certain processing operations without end users' valid consent, within the meaning of the GDPR. The Guidelines explain the elements that gatekeepers should consider in order to comply with the requirements of specific choice and valid consent under Article 5(2) DMA and the GDPR.
- The Guidelines also describe circumstances where consent may not be required by either the GDPR or the DMA and under which conditions other legal bases can be relied upon (e.g. the possibility of relying on Article 6(1), point (c) GDPR when processing personal data for security purposes, provided certain conditions are met).

12. Guidelines 02/2024 on Article 48 GDPR (December 2024)[25]

Article 48 GDPR provides that: "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter".

Relevance:

- The purpose of these guidelines is to clarify the rationale and objective of this article, including its interaction with the other provisions of Chapter V of the GDPR, and to provide practical recommendations for controllers and processors in the EU that may receive requests from third country authorities to disclose or transfer personal data.
- The main objective of the provision is to clarify that judgments or decisions from third country authorities cannot automatically and directly be recognised or enforced in an EU Member State, thus underlining the legal sovereignty vis-a-vis third country law. As a general rule, recognition and enforceability of foreign judgements and decisions is ensured by applicable international agreements.
- Regardless of whether an applicable international agreement exists, if a controller or processor in the EU receives and answers a request from a third country authority for personal data, such data flow is a transfer under the GDPR and must comply with Article 6 and the provisions of Chapter V.

1.3. European Court of Justice Cases

1. La Quadrature du Net (Joined Cases C-511/18, C-512/18, etc.) (2020)[26]

This is an important case, containing decision, which states 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, sabotages on energy infrastructure, etc.) only targeted retention is permitted.

Relevance:

- The Court ruled that Member States cannot cite "national security" to issue blanket mandates for mass data retention. It prevents governments from easily labeling a civilian AI surveillance tool as "national security" just to bypass EU regulations.
- 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.
- 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.
- 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.

2. Ligue des droits humains (Case C-817/19) (2022)[27]

The Court ruled 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.

Relevance:

- The Court imposed strict limitations 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 persons.
- The judgment mandates that any automated match must be subject to an individual human review before any action is taken.

3. SCHUFA Holding AG (Case C-634/21) (Dec 2023)[28]

This is one of the most important cases for the implementation of the project, regarding the automatic risk assessment. The Court ruled that algorithmic scoring which determines decisions falls under GDPR Article 22 restrictions. If a risk score generated by the system leads to significant consequences (e.g., blocking access), it constitutes automated decision-making, requiring human intervention options and stricter GDPR safeguards.

Relevance:

- 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 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.

4. Dun & Bradstreet Austria GmbH (Case C-203/22) (Feb 2025)[29]

This Court case is also very important for some aspects of the project implementation as it is directly related to transparency and automated decisions (so called "Black Box" issue). If the system automatically decides that a certain website or traffic flow is a "threat" and blocks it, according to the Dun & Bradstreet ruling (C-203/22), the user has the right to know the "logic involved" in the decision.

Relevance:

- Individuals have a right to know the "logic involved" in an automated decision. This directly impacts providers of high-risk dual-use AI who might try to hide their algorithms.
- 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, they are entitled to receive "meaningful information about the logic involved".
- 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.
- If a company claims that full disclosure would compromise its 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.

5. EDPS v SRB (C-413/23 P)[30]

The case conserns the aspect pseudonymization. The CJEU in the above-mentioned case 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 institutions, the system should transmit data in a format that the recipient cannot easily link to a specific individual without additional information.

Relevance:

- 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.

6. Deutsche Wohnen (C-807/21)[31]

This case concerns the possible breaches of general data protection rules and implied fines. This CJEU case 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.

Relevance:

- 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 regardingadministrative 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.
- Requirement of Intent or Negligence: Article 83 of Regulation 2016/679 must be interpreted as meaning that an administrative fine may be imposed pursuant to that provision only where it is established that the controller (which is both a legal person and an undertaking) intentionally or negligently committed the infringement referred to in Article 83(4) to (6).

1.4. National policy practices of the Republic of Lithuania

1. Lithuanian Artificial Intelligence Strategy[32].

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.

Relevance:

The strategy emphasizes that Lithuania must further invest in the safety and security advancement of AI technologies, including the explainability, transparency, trust, and resilience of technologies to cyber attacks.

2. National Audit Office. State Audit Report. Management of Artificial Intelligence in the Public Sector (August 2025)[33]

National Audit Office of the Republic of Lithuania prepared a state audit report on management of artificial intelligence in the public sector, which provides important insights on the capabilities of public sector entities to employ the potential of artificial intelligence, including the aspects of cyber security and data protection.

Relevance:

- The state audit determined that effective management of artificial intelligence in the public sector is not yet possible because: appropriate conditions have not been created for the development of this intelligence technology in the public sector, there is a lack of procedures and guidelines for managing artificial intelligence in the public sector, and proper management of the resources necessary for the functioning of artificial intelligence is not ensured.
- There is no national information on artificial intelligence solutions implemented and applied in the public sector, and there is a lack of information on good practices in the application of artificial intelligence in the public sector.
- Artificial intelligence risk mitigation is not ensured through a cybersecurity management system, as there are no special requirements and procedures defining the security of this intelligence throughout its life cycle. When implementing projects related to the application of these technologies in their activities, the majority (81.8%) of public sector entities do not identify and assess the risks of artificial intelligence, none of them conduct an impact assessment and do not have a plan to mitigate this risk.

3. Transposition of NIS2 Directive in Lithuania[34]

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.

Relevance:

- 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.
- The implementing legal acts (e.g., the National Cyber Incident Management Plan35) have been approved, and entities will be registered in the Cybersecurity Entity Register (CISE)36, 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.

4. 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.

Relevance:

- The State Data Protection Inspectorate (SDI) provides detailed guidelines37 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.

1.5. National policy practices of selected EU Member States

France

France's Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), is a key benchmark for providing clear, actionable guidance on reconciling AI development with GDPR principles. This proactive approach offers legal clarity before the AI Act's high-risk systems obligations become fully applicable. CNIL published several recommendations to promote the responsible use of AI while ensuring compliance with personal data protection.

These recommendations confirm that GDPR requirements are sufficiently balanced to address the specific challenges of AI. They provide concrete and proportionate solutions to inform individuals and facilitate the exercise of their rights.

1. CNIL Recommendations on AI and GDPR Compliance[38].

Relevance:

- The recommendations take into account the EU Artificial Intelligence Act recently adopted. Indeed, where personal data is used for the development of an AI system, both the GDPR and the AI Act apply. CNIL's recommendations have therefore been drawn up to supplement them in a consistent manner regarding data protection.

Germany

Germany's strength lies in its long-term strategic integration of cybersecurity into its national AI and industrial policy, particularly emphasizing security-by-design for critical infrastructure.

2. Cyber security strategy for Germany. 2021[39].

The Cyber Security Strategy for Germany 2021 creates a strategic framework for Federal Government policy on cyber security for the next five years, subject to the availability of budgetary funds.

Relevance:

- Cyber Security Strategy sets out four crosscutting guiding principles:
- Establishing cyber security as a joint task for government, private industry, the research community and society.
- Reinforcing the digital sovereignty of government, private industry, the research community and society.
- Making digital transformation secure.
- Setting measurable, transparent objectives.
- The strategic objectives are implemented in three action areas:
  - Action Area 1 – “Remaining safe and autonomous in a digital environment”;
  - Action Area 2 is “Government and private industry working together”;

- Action Area 3 – "Strong and sustainable cyber security architecture for every level of government".

3. The Federal Government's Artificial Intelligence Strategy and AI Action Plan (and related information, programmes, initiatives, etc.)[40].

The Federal Cabinet adopted the Federal Government's Artificial Intelligence Strategy (AI Strategy) in 2018. The AI Strategy is designed to strengthen Germany's position in the international competition for research, development and applications in AI. The AI Strategy is updated to take account of new developments and needs.

Relevance:

- Various different initiatives now focus on the issues of pandemic response, sustainability, environmental protection, climate actionand national and international networking. In 2023 the AI Action Plan was launched as the update to the AI Strategy.

4. The Standard Data Protection Model. A method for Data Protection advising and controlling on the basis of uniform protection goals[41]

The Standard Data Protection Model (SDM) – A method for Data Protection advising and controlling on the basis of uniform protection goals adopted by the Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder on the 24. November 2022 provides appropriate measures to transform the regulatory requirements of the GDPR to qualified technical and organisational measures. For this purpose, the SDM first records the legal requirements of the GDPR and then assigns them to the protection goals Data Minimisation, Availability, Integrity, Confidentiality, Transparency, Unlinkability and Intervenability. The SDM thus transposes the legal requirements of the GDPR on protection goals into the technical and organisationalmeasures required by the Regulation, which are described in detail in the SDM's catalogue of reference measures. It thus supports the transformation of abstract legal requirements into concrete technical and organisational measures.

Relevance:

- The SDM's catalogue of reference measures can be used to check for each individual processing whether the legally required 'target' of measures corresponds to the existing 'actual' of measures.
- The SDM and the catalogue of reference measures also provide a basis for the planning and implementation of the data protection-specific certifications promoted by the GDPR (Art. 42 GDPR) and the data protection impact assessment which is required in certain cases (Art. 35 GDPR).
- Such standardisation also supports the cooperation of supervisory authorities, as stipulated in the Regulation. This also entails that the German data protection authorities increasingly cooperate at national level and that their consulting and testing methods must lead to the same data protection assessments.
- The SDM is created with the aim of providing a coordinated, transparent and verifiable system for data protection assessment. The SDM can also help implement the National E-Government Strategy (NEGS) adopted by the IT-Planning Council in compliance with data protection regulations. The NEGS calls for technical and organisational measures to ensure data protection which respect the principle of data minimisation and that relate to the protection goals of Availability, Confidentiality, Integrity, Transparency, Unlinkability and Intervenability.
- The Standard Data Protection model makes a significant contribution to the effective and legally compliant implementation of the GDPR in Germany as well as in the international context, both for

data protection supervision and for the responsible bodies in the private sector and public administration.

- The SDM enables a systematic and comprehensible comparison between target specifications, which are derived from standards, contracts, declarations of consent and organisational rules, and the current situation resulting from the implementation of these specifications both at organisational and information technology level in the processing of personal data.

The Netherlands

The Netherlands is recognized for its proactive approach to regulating algorithmic risks through its Data Protection Authority (Autoriteit Persoonsgegevens or AP) and its clear vision for institutional cooperation on AI Act enforcement.

Every six months, the Dutch Data Protection Authority (AP) publishes its Report AI & Algorithms Netherlands (RAN). It also draws observations and analyses, based on the knowledge gathered through the network, conversations and consultations with experts and society.

5. AI & algorithmic risks: developments in the Netherlands (and related information, links, initiatives, programmes, etc.)[42].

6. AP and RDI: Supervision of AI systems requires cooperation and must be arranged quickly (and links to related information)[43].

7. Guidelines on AI Literacy[44].

Relevance:

- The use of generative AI raises legal concerns. One aspect of this is the training of models on large quantities of 'scraped' data, which can include personal data. Additionally, new risks for users and the increased concentration of power in big tech firms demand scrutiny.
- Many countries identify large scale spreading of disinformation and manipulation through the use of Generative AI as risks.
- The output of Generative AI is based on probability estimates. The user does often not have insight into uncertainty, plausible alternative answers, or references to origins of the content. This makes it hard to interpret the output and increases the risk of incorrect conclusions and actions. This can result in discrimination and arbitrariness in a person's or organisation's approach.
- The development of generative foundation models takes place at a small number of organisations. Mainly big tech firms have sufficient financial means to invest in this. This makes it hard for new providers to enter the market, and reinforces the existing power of big tech companies.

Denmark

8. Danish Joint Government Digital Strategy.[45]

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.

Relevance:

- 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 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.

9. Visions and recommendations for Denmark as a digital pioneer. Danish government digitization partnership[46]

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.

Relevance:

- 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

10. Finland's Cyber Security Strategy 2024–2035[47]

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.

Relevance:

- 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 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.
- For the project, this confirms a strategic demand for tools that facilitate seamless data exchange between "supervisory authorities" (like Traficom) and "supervised entities" (private enterprises), provided that legislative barriers regarding classified and sensitive information are addressed.
- 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 system 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

11. Sweden in a digital world. A strategy for Sweden's foreign and security policy on cyber and digital issues[48]

Sweden's strategy explicitly positions the private sector as a critical partner in national security, validating the project's aim to deploy a monitoring system for governmental and private organizations.

Relevance:

- 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.
- The document reinforces the importance of the Nordic-Baltic (NB8) region, identifying it as a priority area for deepening cooperation on situational awareness and response to malicious actors like Russia, which supports targeting this region for developed system's initial deployment.

Spain

11. The Spanish Agency for the Supervision of Artificial Intelligence (Guidelines and other relevant information)[49]

The Spanish Agency for the Supervision of Artificial Intelligence is the public body in charge of guaranteeing the ethical and safe use of artificial intelligence in Spain. Its main mission is to ensure that both public and private entities comply with current regulations, protecting privacy, equal treatment and fundamental rights.

AESIA encourages responsible technological development, working in collaboration with other bodies and promoting an environment of trust for the advancement of artificial intelligence, ensuring that it is beneficial and safe for society.

Relevance:

- Guidelines have been developed within the framework of the Spanish AI regulatory sandbox pilot, in collaboration between participants, technical assistants, potential competent national authorities and the sandbox expert advisory group.
- The guide aims to support the implementation and compliance with European Artificial Intelligence regulations and their applicable obligations. Although they are not binding and do not replace or develop the applicable regulations, they provide practical recommendations in line with regulatory requirements pending the approval of harmonised rules for all Member States.

Italy

12. The Agenzia per l'Italia Digitale - Agency for Digital Italy (AgID) (guidelines and other relevant information)[50]

The Agenzia per l'Italia Digitale - Agency for Digital Italy (AgID) - is the technical agency of the Presidency of the Council of Ministers that guarantees the achievement of the objectives of the Italian digital agenda, coordinating all Italian public admnistrations. It also contributes to the diffusion of information and communication technologies, fostering innovation and economic growth. It also promotes digital literacy and its diffusion, in collaboration with institutions as well as international, national and local organizations.

Relevance:

- The Guidelines issued by AgID that set out rules and standards for the implementation of the digital agenda, the digitisation of public administration, IT security, interoperability and application cooperation between public and EU IT systems.

2. Keywords

2.1. Technologies and Systems

- Open Source Operational Technology Sensor (OSOTS)
- Machine Learning (ML)
- Automated cyber defence tools
- Generative AI
- General-purpose AI models

- Network security monitoring software
- Dual-use technologies

2.2. Regulatory Frameworks and Legislation

- General Data Protection Regulation (GDPR)
- AI Act
- Cyber Resilience Act (CRA)
- NIS2 Directive
- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- ePrivacy Directive
- Defence Readiness Omnibus
- Digital Omnibus

2.3. Compliance and Operational Principles

- Security by Design
- Privacy by Design
- Data minimization
- Pseudonymisation
- Human oversight
- Automated individual decision-making
- Risk-based approach
- Data Protection Impact Assessment (DPIA)
- Right to an explanation
- Transparency
- Standard Data Protection Model (SDM)

2.4. Threats and Security Context

- Hybrid threats
- Critical infrastructure
- Cyber incident detection and response
- Disinformation
- National security
- Adversarial AI

2.5. Strategic and Institutional Terms

- European Defence Industrial Strategy (EDIS)
- NATO Principles of Responsible Use
- Data Strategy for the Alliance
- Apply AI Strategy
- Public-private partnerships
- European Data Protection Board (EDPB),
- Court of Justice of the European Union (CJEU)

Conclusions

1. General conclusions

Strategic Alignment with EU and NATO Priorities

- The project is highly relevant to the current geopolitical climate, addressing the urgent shortage of cybersecurity skills through automation and Machine Learning (ML). It aligns directly with the European Defence Industrial Strategy (EDIS) and NATO's focus on Emerging and Disruptive Technologies (EDTs), which prioritize technological supremacy in AI and cybersecurity to counter hybrid threats and protect critical infrastructure. The project fits the "dual-use" definition, bridging the gap between civilian innovation and defense needs, a synergy explicitly encouraged by the European Commission to enhance regional security and competitiveness.

The Inseparability of "Security by Design" and Compliance

- Regulatory compliance is not merely an administrative hurdle but a foundational architectural requirement. The Cyber Resilience Act (CRA) and Union Rolling Work Programme make "Security by Design" and "Data Minimization" non-negotiable for obtaining European certification. Furthermore, the system must navigate a complex interplay of regulations:
    - GDPR & Privacy: The system must strictly adhere to data minimization (collecting only essentials like headers) and pseudonymization principles.
    - AI Act: The system acts as a high-risk tool. It must avoid "prohibited practices" (unacceptable risk) and ensure transparency.
    - NIS2 Directive: In Lithuania and Finland, the transposition of NIS2 creates a legal mandate for information sharing and stronger resilience in critical sectors, validating the need for this sensor.

Legal Risks of Automated Decision-Making

- The most significant legal hurdles stem from the system's potential to automatically block threats. Court of Justice of the European Union (CJEU) rulings have established strict boundaries:
- Human Oversight is Mandatory: Automated systems cannot be the sole arbiter of significant decisions (like blocking access) without human review (Ligue des droits humains, SCHUFA).
- Right to Explanation: Users have a right to understand the "logic involved" in an automated decision. "Black box" algorithms that cannot explain why a traffic flow was flagged are legally vulnerable (Dun & Bradstreet).
- Mass Surveillance Constraints: General and indiscriminate retention of traffic data is prohibited unless there is a specific, genuine threat to national security (La Quadrature du Net).

2. Recommendations

Technical and Architectural Recommendations

- Implement "Dual-Use by Design": Develop the software architecture to serve both civilian and military objectives from the outset. This ensures eligibility for defense funding (like the European Defence Fund) while remaining commercially viable for critical infrastructure sectors.

- Adopt the Standard Data Protection Model (SDM): Utilize the German SDM methodology to translate abstract legal requirements (integrity, unlinkability, transparency) into concrete technical measures. This provides a verifiable system for data protection assessment and certification.
- Enforce Strict Data Minimization: Configure the sensor to collect only the "bare essentials" needed for threat detection (e.g., metadata/headers rather than full packet content) to comply with the Union Rolling Work Programme and GDPR.

Legal and Operational Governance

- Mandate Human-in-the-Loop (HITL): Design the incident response workflow so that the ML algorithm acts as a decision-support tool rather than a fully autonomous agent for critical actions. A human operator must review automated "risk scores" before significant punitive actions (like permanent blocking) are taken, complying with SCHUFA and Ligue des droits humains rulings.
- Ensure Algorithmic Transparency: To satisfy the Dun & Bradstreet ruling, the system must be able to generate an intelligible explanation of why a specific anomaly was flagged. Avoid proprietary "black box" models that cannot provide the "key parameters" of the decision logic to the user.
- Conduct Data Protection Impact Assessments (DPIA): Given the use of ML and the potential monitoring of public/private networks, a DPIA is mandatory. This must assess risks related to automated decision-making and potential bias.

Strategic Implementation and Partnerships

- Pursue European Cybersecurity Certification: Aim for certification under the CRA framework. This serves as a "passport" for the product to operate across all EU member states without navigating fragmented national laws.
- Leverage Public-Private Partnerships: Follow the Finnish and Swedish models by creating trust-based information-sharing channels. The system should facilitate data exchange between "supervisory authorities" and private enterprises, addressing the fragmentation noted in national strategies.
- Address Public Sector Readiness (Lithuania specific): Since the Lithuanian public sector currently lacks AI risk mitigation procedures, provide a "turnkey" compliance module with the sensor that includes pre-packaged risk assessment templates and training materials to help public entities meet their NIS2 and AI management obligations.

References

1. Union Rolling Work Programme for European cybersecurity certification. https://ec.europa.eu/newsroom/dae/redirection/document/102292
2. 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
3. White paper on options for enhancing support for research and development involving technologies with dual-use potentialCOM(2024) 27 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0027
4. 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

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. European Commission. European approach to artificial intelligence, policy review (2025). https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
8. The AI Continent Action Plan. https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan
9. 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
10. 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
11. Defence Readiness Omnibus. Simplification proposal to boost industrial readiness. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-readiness-omnibus_en
12. Digital Omnibus proposal. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal
13. The Helsinki Statement on enhanced clarity, support and engagement (July 2025): https://www.edpb.europa.eu/system/files/2025-07/edpb-statement-20250702-enhanced-clarity-support-engagement_en_0.pdf
14. 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
15. 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
16. 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
17. Guidelines 01/2025 on Pseudonymisation: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf
18. Guidelines 3/2025 on the interplay between the DSA and the GDPR (September, 2025): https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf
19. Orientations on generative Artificial Intelligence (generative AI) and personal data protection (September 2025): https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf
20. Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (October 2024): https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf
21. The General-Purpose AI Code of Practice: https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
22. First Draft Code of Practice on Transparency of AI-Generated Content: https://ec.europa.eu/newsroom/dae/redirection/document/123074
23. Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act): https://ec.europa.eu/newsroom/dae/redirection/document/112455
24. Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation: https://www.edpb.europa.eu/system/files/2025-10/joint_com-edpb_gls_interplay_dma_gdpr_for_public_consultation_en.pdf

25. Guidelines 02/2024 on Article 48 GDPR (December 2024): https://www.edpb.europa.eu/system/files/2024-12/edpb_guidelines_202402_article48_en.pdf
26. C-511/18 - La Quadrature du Net and Others. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
27. C-817/19 - Ligue des droits humains. https://curia.europa.eu/juris/liste.jsf?num=C-817/19
28. Case C-634/21 - SCHUFA Holding AG. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
29. Case C-203/22 - Dun & Bradstreet Austria GmbH. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
30. 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
31. 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
32. Lithuanian Artificial Intelligence Strategy. https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf
33. National Audit Office. State Audit Report. Management of Artificial Intelligence in the Public Sector (August 2025): https://www.valstybeskontrole.lt/LT/Product/Download/4871
34. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
35. National Cyber Incident Management Plan of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
36. Cybersecurity Entity Register (CISE). https://www.nksc.lt/ksis
37. The State Data Protection Inspectorate of the Republic of Lithuania. Guidelines. https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/work/
38. CNIL Recommendations on AI and GDPR Compliance. https://www.cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-support-responsible-innovation and https://www.cnil.fr/en/ai-how-comply-regulations
39. Cyber security strategy for Germany. 2021. https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4
40. The Federal Government's Artificial Intelligence Strategy and AI Action Plan (and related information, programmes, initiatives, etc.). https://www.bmftr.bund.de/EN/Research/EmergingTechnologies/ArtificialIntelligence/artificialintelligence_node.html andhttps://www.bmftr.bund.de/DE/Forschung/Schluesseltechnologien/KuenstlicheIntelligenz/KiAktionsplan/kiaktionsplan_node.html
41. The Standard Data Protection Model. A method for Data Protection advising and controlling on the basis of uniform protection goals: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM_V3_en.pdf
42. AI & algorithmic risks: developments in the Netherlands (and related information, links, initiatives, programmes, etc.). https://www.autoriteitpersoonsgegevens.nl/en/themes/algorithms-ai/ai-algorithmic-risks-developments-in-the-netherlands
43. AP and RDI: Supervision of AI systems requires cooperation and must be arranged quickly (and links to related information). https://www.autoriteitpersoonsgegevens.nl/en/current/ap-and-rdi-supervision-of-ai-systems-requires-cooperation-and-must-be-arranged-quickly
44. Guidelines on AI Literacy. https://www.autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-ai-geletterdheid
45. Danish Joint Government Digital Strategy. https://en.digst.dk/strategy/the-joint-government-digital-strategy/

46. 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
47. Finland's Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content
48. 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
49. The Spanish Agency for the Supervision of Artificial Intelligence (Guidelines and other relevant information): https://aesia.digital.gob.es/en/guides
50. The Agenzia per l'Italia Digitale - Agency for Digital Italy (AgID) (guidelines and other relevant information): https://www.agid.gov.it/en/guidelines

ANNEX 2
CASE STUDIES

1. Hypothetical Case Study: Implementation of the OSOTS Project

1.1. Analysis of the Regulatory Environment (EU/NATO)

The OSOTS project operates at the intersection of critical infrastructure protection and "dual-use" technology (civilian and defense). The regulatory environment requires a "Security by Design" approach where compliance is architectural, not just administrative.

A. European Union Framework

- General Data Protection Regulation (GDPR)1: The project must adhere strictly to data minimization(collecting only essentials like headers) and pseudonymization. A critical restriction involves Automated Individual Decision-Making (Article 22). Recent CJEU rulings (SCHUFA2, Ligue des droits humains3) establish that if the sensor's risk score decisively influences actions (like blocking a user), it constitutes an automated decision requiring human intervention and strict safeguards.
- The AI Act4: OSOTS is likely a high-risk system as it is a "cyber threat management system" for critical infrastructure. It must avoid "prohibited practices" (unacceptable risk) and ensure transparency. Users have a "right to an explanation" regarding the logic of the AI, meaning "black box" algorithms are legally vulnerable (Dun & Bradstreet ruling5).
- NIS2 Directive6: Transposed into national laws (e.g., in Lithuania), this mandates rigorous incident reporting and information sharing for critical entities (energy, water, etc.). The sensor must facilitatecompliance with these reporting obligations.
- Cyber Resilience Act (CRA)7: This acts as a "passport" for the product. Certification under the CRA requires "Security by Design" and careful vulnerability handling throughout the software lifecycle.

B. NATO & Defense Framework

- Dual-Use & Interoperability: The European Defence Industrial Strategy (EDIS)8 and NATO's policy on Emerging and Disruptive Technologies (EDTs)9 encourage "dual-use by design". This means the software should bridge civilian innovation and military needs.
- Data Strategy: NATO emphasizes "Data Centric Reference Architecture" and compliance with international law, requiring systems to balance the "responsibility to share" with "need-to-know" principles.

1.2. Compliance Mapping

This checklist maps specific project actions to legal provisions referenced in the sources of this case study.

Category	Requirement	Legal Reference / Source
Data Privacy (GDPR)	**Data Minimization:** Configure sensor to capture only metadata/headers, not full packet content, unless strictly necessary.	**Union Rolling Work Programme[10]; GDPR Art. 5(1)(c).**
	Prohibition on General Retention: Ensure no indiscriminate mass retention of traffic data; retention must be targeted or based on genuine threats.	**CJEU Case *La Quadrature du Net*[11].**

	Automated Decision Limits: If the sensor blocks traffic automatically, it must not be the sole arbiter if consequences are significant.	**GDPR Art. 22**; **CJEU Case *SCHUFA***.
	Right to Explanation: The system must explain the "key parameters" of why a threat was flagged (no "black box").	**CJEU Case *Dun & Bradstreet***.
AI Governance	**Prohibited Practices:** Verify the ML model does not use techniques labeled as "unacceptable risk" (e.g., manipulative techniques).	**AI Act**; **Commission Guidelines**[12].
	Human Oversight: Implement "Human-in-the-Loop" (HITL) workflows where operators review AI flags before severe actions.	**CJEU Case *Ligue des droits humains***.
	Transparency: Mark AI-generated content/decisions clearly.	**AI Act Art. 53**; **GPAI Code of Practice**[13].
Cybersecurity	**Security by Design:** Integrate security measures from the first design phase, not as an add-on.	**Union Rolling Work Programme**; **NATO EDT Strategy**.
	Incident Reporting: Ensure the system generates data formats compatible with NIS2 reporting requirements for CSIRTs.	**NIS2 Directive**; **Lithuanian Law on Cybersecurity**[14].
Defense/Dual-Use	**Interoperability:** Align with NATO standards (e.g., STANAG 5636) to ensure data can be shared securely across alliances.	**NATO Data Strategy**[15]; **EDIS**.

1.3. Most Important Stages of Implementation

Based on the "Security by Design" and "Dual-Use by Design" principles, the four crucial stages are:

1. Architectural Design & Risk Assessment: The foundational stage where legal requirements are translated into code logic.
2. Data Processing & Model Training: Developing the ML models while strictly managing personal data and bias.
3. Operational Deployment (The "Sensor" in Action): The active monitoring phase where the system interacts with live network traffic.
4. Incident Management & Response: The post-detection phase involving reporting and information sharing.

1.4. Practical Steps for Each Stage

Stage 1: Architectural Design & Risk Assessment

- Conduct a DPIA: Perform a Data Protection Impact Assessment (DPIA) immediately. This is mandatory for AI systems monitoring public/private networks.
- Define "Dual-Use" Scope: Design the software to serve both civilian critical infrastructure and potential defense needs to qualify for funding (e.g., European Defence Fund).
- Adopt Standard Data Protection Model (SDM): Use the German SDM methodology16 to translate abstract legal goals (integrity, unlinkability) into concrete technical specifications.

Stage 2: Data Processing & Model Training

- Pseudonymization by Default: Implement pseudonymization domains to determine who can attribute data to individuals. Ensure the recipient (e.g., a central authority) cannot re-identify subjects without additionalinformation.
- Bias Detection: If processing special categories of data is necessary for bias detection (to ensure the AI doesn't discriminate), apply strict safeguards as permitted by the Apply AI Strategy.17
- Avoid "Black Box" Models: Select ML algorithms that allow for interpretability. You must be able to provide "meaningful information about the logic involved" to satisfy the Dun & Bradstreet ruling.

Stage 3: Operational Deployment

- Configure "Targeted" Retention: Do not set the sensor to retain all traffic data indefinitely. Configure itfor targeted retention (specific risk triggers or geographic areas) to comply with La Quadrature du Net.
- Implement Human-in-the-Loop (HITL): Design the dashboard so the AI acts as a decision-support tool. A human operator must validate "high consequence" alerts (e.g., blocking a subnet) to avoid Article 22 GDPR violations.
- Liability Protection: Ensure the system logs prove that "necessary security measures" were active. Fines are imposed only for "intent or negligence" (Deutsche Wohnen18 case); robust logs protect the operator from liability during unavoidable incidents.

Stage 4: Incident Management & Response

- Automated NIS2 Reporting: Build features that automatically format incident data for submission to national authorities (like the NCSC in Lithuania)19.
- Trust-Based Sharing: Facilitate data exchange between the "supervisory authority" and the "supervised entity" (private sector), a gap identified in Finland's20 and Sweden's21 strategies.
- Cross-Border Formats: Use standard data formats (NATO STANAGs) to allow potential sharing with EU/NATO allies if the threat is hybrid or state-sponsored.

1.5. Practical Challenges Due to Lack of Legal Clarity

A. The "Black Box" vs. Transparency Paradox

- Challenge: The Dun & Bradstreet ruling entitles users to know the "logic involved" in automated decisions. However, revealing the full source code or weights of a security ML model could compromise its effectiveness against attackers or reveal proprietary trade secrets.
- Ambiguity: The courts suggest a "balancing exercise," but it is unclear exactly how much detail (e.g., "key parameters") is sufficient to satisfy the user without breaking security.

B. Data Retention in "Peace" vs. "Hybrid Threat" Scenarios

- Challenge: La Quadrature du Net prohibits general mass surveillance unless there is a "genuine and present" national security threat.
- Ambiguity: In the context of "hybrid threats" (e.g., sabotage of energy infrastructure mentioned in), the line between "crime fighting" (targeted retention) and "national security" (general retention allowed) is blurred. Operators may struggle to know when they can legally switch to "full capture" mode without a formal government declaration of emergency.

C. The Definition of "Automated Decision"

- Challenge: Under SCHUFA, a score that "decisively influences" a decision is an automated decision.
- Ambiguity: If the OSOTS sensor provides a "risk score" of 99% and the human operator always follows the recommendation because they lack the time to investigate, does this

legally become a prohibited "automated decision" due to the "automation bias" of the human? The legal threshold for "meaningful" human review remains subjective in operational reality.

D. Civilian vs. Defense Data Sharing

- Challenge: While the Defence Readiness Omnibus22 aims to simplify dual-use transfers, current national laws (e.g., in Finland) still struggle with decentralized regulations that hinder information sharing between private entities and intelligence agencies.
- Ambiguity: It is often unclear if a private operator of a solar farm (civilian) can legally share un-anonymized threat data with military cyber defense units under GDPR.

2. Real-World Case Analysis

There are several commercial ventures that offer similar but not identical products, like Nozomi Guardian, Forescout, Dragos, Claroty. Some of the existing products are distributed in non-EU markets, which results in a different regulatory environment. Case studies of these market participants are discussed here to the extent that they relate to publicly available and unclassified information. Here is a detailed analysis of Nozomi Networks**,** Forescout**,** Dragos**,** and Claroty**.** This analysis applies the criteria established in your previous query regardingthe OSOTS project - specifically focusing on regulatory compliance (GDPR/EU), architecture (Cloud/On-prem), AI governance, and practical implementation for cyber-physical systems (CPS).

2.1. Nozomi Networks

Product Focus: Operational Resilience and Deep Visibility (Guardian & Vantage)[23].

- **Architecture & Implementation:**
  - Hybrid Deployment: Nozomi offers a flexible architecture comprising Guardian sensors (physical or virtual) that sit at the edge, and Vantage, a cloud-based SaaS management console. For organizations with strict data sovereignty requirements (e.g., classified defense networks), they offer an on-premises Central Management Console (CMC), allowing for an air-gapped architecture.
  - Discovery Method: Primarily uses passive monitoring (Deep Packet Inspection) to ensure "do no harm" to sensitive OT equipment. However, they augment this with "Smart Polling," a low-volume active querying technique to identify non-communicating or "silent" assets, ensuring a comprehensive inventory.
  - Wireless Monitoring: A unique differentiator is Guardian Air, which monitors wireless frequencies (Bluetooth, Zigbee, LoRaWAN) to detect rogue devices that bypass wired sensors, a critical feature for modern "hybrid" threat landscapes.

- **Compliance (GDPR & NIS2):**
  - Data Minimization: Guardian sensors process data locally. "Asset Intelligence" anonymizes data to update threat profiles without exposing sensitive user data to the cloud.
  - NIS2 Reporting: The platform includes specific compliance modules for NERC CIP and the NIS2 Directive, facilitating the mandatory incident reporting required by EU law.
  - Data Integrity: Recent updates (N2OS v24.6) enforce the use of the ZFS filesystem to ensure higher data integrity and reliability for stored logs, critical for forensic audit trails required by legal standards.

- **AI & Threat Detection (AI Act):**

- Behavioral Baselining: Nozomi uses AI to learn "normal" process variable states (e.g., standard RPMs for a turbine). It creates a baseline and alerts only on deviations, reducing "alert fatigue".
- AI Governance: The "Asset Intelligence" engine is trained on millions of global assets to reduce false positives. New features include "Alert Deduplication" using advanced logic to group incidents, simplifying the human oversight required by high-risk AI systems.

2.2. Forescout Technologies

Product Focus: Universal Zero Trust & Active Enforcement (The 4D Platform)[24].

- **Architecture & Implementation:**
  - IT/OT Convergence: Forescout distinguishes itself by bridging the gap between IT and OT. Unlike pure-play OT vendors, it offers Network Access Control (NAC) capabilities, allowing it to not just detect but actively block or segment devices based on policy.
  - Agentless Discovery: It utilizes over 30 active and passive techniques to classify devices without installing software agents, which is essential for "unmanageable" IoT/OT devices.
  - Deployment: Offers flexible options including on-premises appliances, virtual machines, and the cloud-native eyeSentry for exposure management.

- **Compliance (GDPR & NIS2):**
  - Segmentation for Privacy: Its strong segmentation capabilities (eyeSegment) allow organizations to dynamically isolate sensitive data streams, aiding in GDPR compliance by enforcing "integrity and confidentiality" at the network layer.
  - Risk Compliance: The platform aligns with the NIST Cybersecurity Framework and IEC 62443, helping organizations meet the "state of the art" security measures required by the EU NIS2 Directive.

- **AI & Threat Detection (AI Act):**
  - Vedere Labs Intelligence: The platform is powered by the "Device Cloud," a repository of 19 million analyzed devices. It uses "True Threat Correlation" to distinguish between operational errors and cyberattacks.
  - Risk Scoring: Forescout calculates a multifactor risk score based on configuration, behavior, and function. This quantitative approach aligns with the risk-based requirements of modern cyber regulations.

2.3. Dragos

Product Focus: Threat Intelligence & Incident Response (Dragos Platform 3.0)[25].

- **Architecture & Implementation:**
  - Defender-Centric: Founded by intelligence community veterans, Dragos focuses heavily on "codifying" human expertise into the software. The platform includes expert-authored playbooks that guide analysts step-by-step through an incident.
  - Platform 3.0: The latest version introduces the "Insights Hub," a unified dashboard that consolidates vulnerabilities and threats into a prioritized view to speed up "time-to-value".
  - Hardware: Offers ruggedized hardware (e.g., STS-50) for harsh industrial environments, ensuring physical resilience.

- **Compliance (GDPR & NIS2):**

- Collective Defense (Privacy-Preserving): Dragos offers "Neighborhood Keeper," a collective defense network that allows participants to share threat intelligence anonymously. This architecture is designed to share threat data without sharing personal data or proprietary topology, adhering to strict privacy standards.
- Vulnerability Management: Uses a "Now, Next, Never" prioritization framework. This helps operators focus compliance efforts on the 6% of vulnerabilities that are actually exploitable, optimizing resource allocation for NIS2 compliance.

- **AI & Threat Detection (AI Act):**
  - Augmented Intelligence: Dragos explicitly states that AI is used to "augment, not replace, human expertise." Platform 3.0 uses AI to accelerate back-end vulnerability analysis but keeps humans in the loop for critical decisions, a "Human-in-the-Loop" approach favored by EU regulation.

2.4. Claroty

Product Focus: Unified Cyber-Physical Systems Protection (xDome & CTD)[26].

- **Architecture & Implementation:**
  - Dual-Mode Deployment: Claroty offers xDome (SaaS/Cloud) for enterprise scalability and Continuous Threat Detection (CTD) (On-Premises) for strictly air-gapped environments.
  - Secure Access: Unlike competitors that focus primarily on monitoring, Claroty includes a built-in Secure Access (formerly SRA) module to manage remote vendor access - a critical requirement for NIS2 supply chain security.
  - Specialization: Highly specialized in healthcare (IoMT) through its Medigate acquisition, managing clinical workflows and patient safety alongside standard industrial security.

- **Compliance (GDPR & NIS2):**
  - Safe Queries: Claroty uses a proprietary "Safe Query" technology that actively polls devices without crashing them, ensuring an accurate asset inventory (GDPR Article 30: Record of Processing Activities) without disrupting operations.
  - Data Sovereignty: The CTD on-premise option ensures that sensitive critical infrastructure data never leaves the facility, satisfying the strictest national security and data residency laws.

- **AI & Threat Detection (AI Act):**
  - CPS Library: In late 2025, Claroty released the "CPS Library," powered by Large Language Models (LLMs) and statistical inference. It utilizes Generative AI to categorize assets and map vulnerabilities with high precision.
  - Resilient Detection: The platform uses a "resilient detection model" that correlates alerts with business impact, allowing organizations to prioritize based on financial risk.

2.5. Comparative summary

A. Comparative Summary Table

Feature	NozomiNetworks	Forescout	Dragos	Claroty
Primary Deployment	Hybrid (Guardian + Vantage Cloud)	Hybrid (4D Platform + eyeSentry)	On-Prem Focus (Platform 3.0)	Hybrid (xDomeCloud + CTD On-Prem)

Asset Discovery	Passive + "Smart Polling" + Wireless (Guardian Air)	Agentless (30+ active/passive techniques)	Passive + Active Collection + Agent (LWC)	Passive + "Safe Queries" + Edge Collector
Key Differentiator	**Operational Resilience:** Best visualization & wireless monitoring.	**Enforcement:**Integrated NAC to actively block/segment threats.	**Intelligence:**"Neighborhood Keeper" & expert playbooks.	**CPS Breadth:**Strongest Healthcare/IoMTfocus & Remote Access.
AI Approach	Behavioral baselining & Alert Deduplication.	Risk Scoring & "True Threat Correlation".	AI-enhanced vulnerability analysis (Human-in-the-loop).	GenAI-powered "CPS Library" for asset ID.
GDPR/Privacy	Anonymized Asset Intelligence.	Segmentation for data privacy.	Anonymous collective defense sharing.	On-prem options for strict sovereignty.

B. Practical Challenges for All Vendors

A common challenge identified across all four vendors is the cost and complexity of deployment.

- Forescout is noted for higher licensing costs due to its per-endpoint model.
- Nozomi requires add-on licenses for features like "Smart Polling," increasing TCO.
- Dragos is positioned as a premium, defender-focused solution that may be resource-intensive for smaller teams.
- Claroty faces challenges in integrating with legacy proprietary protocols in highly complex environments.

Each solution is moving toward **"Platformization"** - consolidating visibility, risk, and response into a single pane of glass to meet the comprehensive security requirements of the NIS2 Directive and the Cyber Resilience Act.

Based on the comparative analysis of **Nozomi Networks**, **Forescout**, **Dragos**, and **Claroty**, the primary challenge facing these organizations is navigating the technical and operational complexity of converging IT and OT environments while managing high costs and deployment friction. **Forescout**, while powerful in network enforcement, faces criticism regarding the complexity of its deployment and user interface, which requires significant tuning to minimize false positives and effectively manage dual-homed devices. Similarly, while **Claroty** and **Nozomi Networks** are praised for their visibility, they face hurdles in integrating seamlessly with legacy proprietary protocols in multi-vendor environments, and recent technical shifts - such as Nozomi'sdeprecation of support for older virtualization standards - have forced customers into complex hardware and software upgrade cycles to maintain support.

Financially and strategically, all four vendors struggle with the perception of high total cost of ownership (TCO) and resource intensity. **Dragos** is explicitly positioned as a "premium," defender-centric solution, which creates barriers for smaller organizations or those outside its primary North American critical infrastructure market due to its high price point and heavy reliance on on-premises resources. **Claroty** and **Forescout** also face resistance regarding their licensing models, with users noting that scaling protection across thousands of endpoints becomes prohibitively expensive. Furthermore, as the market shifts from passive monitoring to active defense, these vendors are challenged to implement "active" querying techniques (like Claroty's Safe Queries or Nozomi's Smart Polling) that provide deep data without disrupting fragile industrial processes, a delicate balance that remains a source of operational anxiety for asset owners.

ANNEX: Detailed Compliance and Implementation Checklist for OSOTS

1. Data Protection & Privacy Architecture (GDPR Focus)

Objective: Ensure the sensor's architecture respects fundamental rights while monitoring traffic, complying with strict CJEU case law regarding mass surveillance and automated processing.

A. Data Processing & Retention

- **Implement Targeted Retention Policies:**
  - Requirement: Do not configure the sensor for "general and indiscriminate retention" of traffic data.
  - Action: Configure the system to default to "targeted retention" (e.g., specific geographic areas, IP ranges, or timeframes) triggered only by specific threat indicators. General retention is legally permissible only during a "genuine and present" national security threat.
- **Enforce Data Minimization (Headers vs. Payload):**
  - Requirement: Collect only the "bare essentials."
  - Action: By default, restrict data capture to packet headers and metadata. Full packet content inspection should be an optional, temporary escalation state, not the default mode.
- **Pseudonymization Strategy:**
  - Requirement: Ensure unlinkability where possible.
  - Action: Implement "pseudonymization domains" so that the entity analyzing the data (e.g., a central CSIRT) cannot re-identify specific users without additional information held separately. Ensure the recipient of shared data cannot legally or technically re-identify the subject.

B. Automated Decision-Making (ADM) Safeguards

- **Human-in-the-Loop (HITL) Workflow:**
  - Requirement: Prevent Article 22 GDPR violations regarding automated decisions with significant effects.
  - Action: Design the dashboard as a Decision Support System. The AI provides a "risk score," but a human operator must validate "high consequence" actions (e.g., permanently blocking a subnet). The system must not be the sole arbiter.
- **Algorithmic Transparency (The "Black Box" Test):**
  - Requirement: Users have a "right to an explanation" of the logic involved in automated decisions.
  - Action: Ensure the ML model can output the "key parameters" that led to a specific alert (e.g., "Flagged due to unusual port scanning frequency at 03:00 AM"). Avoid fully opaque "black box" models that cannot explain their logic to a human, as this violates rights established in the Dun & Bradstreet ruling.
- **Legitimate Interest Assessment (LIA):**
  - Requirement: Balance security needs with user rights.
  - Action: Before deployment, conduct a documented assessment proving that the monitoring is "necessary" and that the security goal cannot be achieved by less intrusive means.

2. Artificial Intelligence Governance (AI Act & Ethics)

Objective: Align the Machine Learning (ML) components with the EU AI Act's "High-Risk" requirements and "Prohibited Practices."

- **Prohibited Practices Screening:**
  - Requirement: Ensure no "unacceptable risk" features.
  - Action: Audit the code to ensure the sensor does not use manipulative techniques or exploit vulnerabilities of specific groups. Verify the system does not engage in "social scoring".

- **Bias Detection & Mitigation:**
  - Requirement: Prevent discriminatory outcomes in threat detection.
  - Action: If processing special categories of data is required to detect bias (e.g., ensuring the AI doesn't unfairly flag traffic from specific regions), use the "regulatory sandbox" or specific legal exemptions allowed for bias testing under strict safeguards.
- **AI System Definition & Registration:**
  - Requirement: Clarify legal status.
  - Action: Assess if the software meets the definition of an "AI System" under Article 3(1) of the AI Act (inference, autonomy). If yes, prepare for registration in the EU database for high-risk systems.
- **Generative AI Content Marking (If applicable):**
  - Requirement: Transparency for AI-generated reports.
  - Action: If the sensor uses GenAI to write incident reports, these outputs must be machine-readable and clearly marked as AI-generated.

3. Cybersecurity & Resilience (NIS2, CRA, NATO)

Objective: Ensure the product is secure by design and interoperable with EU/NATO defense standards.

- **Security by Design & Certification:**
  - Requirement: Integrate security from the first design phase.
  - Action: Adopt the "Secure Development Lifecycle" (SDL). Prepare the software for certification under the Cyber Resilience Act (CRA) to serve as a "passport" for the EU market.
- **Standard Data Protection Model (SDM):**
  - Requirement: Transform abstract legal goals into technical specs.
  - Action: Adopt the German SDM methodology to map GDPR goals (Availability, Integrity, Confidentiality, Unlinkability) to specific technical configurations in the sensor code.
- **Interoperability & Data Formats:**
  - Requirement: Facilitate information sharing.
  - Action: Use data formats compatible with NATO STANAG 5636 and the "Data Centric Reference Architecture" (DCRA). This ensures the sensor can share intelligence with allies if the threat is identified as a hybrid/state-sponsored attack.
- **Incident Reporting Automation:**
  - Requirement: NIS2 compliance.
  - Action: Build features that automatically format logs into reports required by national CSIRTs (like the NCSC in Lithuania), reducing the burden on the operator.

4. Organizational & National Implementation

Objective: Address specific national requirements and organizational readiness gaps.

- **Liability & Logging:**
  - Requirement: Protection against fines.
  - Action: Ensure the system maintains immutable logs of all security measures taken. Liability/fines usually require "intent or negligence"; robust logs prove diligence.
- **Public Sector Readiness Kit (Lithuania Focus):**
  - Requirement: Address the "lack of procedures" in the public sector.
  - Action: Since 81.8% of Lithuanian public entities lack AI risk assessments, bundle the OSOTS sensor with a "compliance kit" (templates for DPIA, risk assessment) to help them meet national audit requirements.

- **Dual-Use Funding Eligibility:**
  - Requirement: Bridge Civil-Defense gaps.
  - Action: Explicitly document the "dual-use" nature of the technology (civilian critical infra protection + military defense) to qualify for funding under the European Defence Fund (EDF) and the "Defence Readiness Omnibus".
- **Trust-Based Sharing Protocols:**
  - Requirement: Enable public-private cooperation.
  - Action: Implement protocols that allow "supervised entities" (private companies) to share threat data with "supervisory authorities" without fear of leaking trade secrets, following the Finnish/Swedish comprehensive security models.

References

1. General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
2. CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
3. CJEU Case C-817/19 - Ligue des droits humains. https://curia.europa.eu/juris/liste.jsf?num=C-817/19
4. Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
5. CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
6. NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
7. Cyber Resilience Act. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847
8. Joint Communication. European Defence Industrial Strategy (EDIS) (March 2024). https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=EDIS%20Joint%20Communication.pdf
9. Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies (EDTs) (February 2021). https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies
10. Union Rolling Work Programme for European cybersecurity certification. https://ec.europa.eu/newsroom/dae/redirection/document/102292
11. CJEU Case C-511/18 - La Quadrature du Net and Others, 2020. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
12. Guidelines on prohibited artificial intelligence (AI) practices. February 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act
13. The General-Purpose AI Code of Practice: https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
14. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
15. Data Strategy for the Alliance (May 2025). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance
16. The Standard Data Protection Model. A method for Data Protection advising and controlling on the basis ofuniform protection goals: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM_V3_en.pdf
17. Apply AI Strategy (COMMUNICATION FROM THE COMMISSION Artificial Intelligence for Europe) COM(2025) 723 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0723

18. CJEU Case C-807/21 - Deutsche Wohnen, 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=282192&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8123480
19. Cybersecurity Entity Register (CISE). https://www.nksc.lt/ksis
20. Finland's Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content
21. Sweden in a digital world. A strategy for Sweden's foreign and security policy on cyber and digital issues. https://www.government.se/contentassets/f858cec8cb944d3fa82bdf0fb7959448/sweden-in-a-digital-world---a-strategy-for-swedens-foreign-and-security-policy-on-cyber-and-digital-issues.pdf
22. Defence Readiness Omnibus. Simplification proposal to boost industrial readiness. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-readiness-omnibus_en
23. Nozomi Networks. https://www.nozominetworks.com/
24. Forescout Technologies. https://www.forescout.com/
25. Dragos. https://www.dragos.com/
26. Claroty. https://claroty.com/