Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

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

Project name: ***EPMwDC***

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

Action result: ***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)
Saulius Kvedaravičius (MRU)

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

Executive Summary

This report provides a regulatory and risk-based analysis of the EPMwDC system, a dual-use hardware and software solution intended to prevent unauthorised visual capture of sensitive screen content through preventative, detective, reporting and remote monitoring functions. The analysis focuses on the regulatory domains most relevant to the system's design and deployment, namely cybersecurity, data protection, artificial intelligence governance, classified-information protection, defence and national security requirements, and dual-use controls.

The report shows that the system cannot be assessed as a purely technical security tool – its compliance must be considered across the full system lifecycle. The main conclusion is that the system's legal classification and related obligations depend heavily on its deployment context. The same technology may be subject to different requirements when used in civilian, governmental, law enforcement, defence or classified environments.

The report also identifies key technical, operational and regulatory risks as well as related mitigation measures. Overall, the analysis establishes a structured framework for translating legal and regulatory requirements into concrete design, deployment and governance measures for the EPMwDC and likewise system.

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

Introduction

This document provides an analysis of the regulatory and standards requirements applicable to the Espionage Prevention Monitor with Detection Capabilities (**EPMwDC**) project and comparable systems intended for deployment within sensitive, security-critical and defence-related environments. The EPMwDC system, consisting of integrated hardware and software components, is designed to support the prevention of unauthorised disclosure of sensitive information through the detection, recording and reporting of attempts to capture confidential or protected data displayed on secured devices, workstations, or information systems.

The purpose of this document is to identify and consolidate the regulatory requirements such as concerning cyber security, data protection and other fields, relevant to the design, development, deployment, operation and maintenance of the EPMwDC and likewise solutions. Attention is given to obligations arising under different regulatory systems such as applicable European Union (**EU**), North Atlantic Treaty Organisation (**NATO**), European Defence Agency (**EDA**) frameworks. While this document aims to address the applicable framework comprehensively, it is not intended to provide a full compliance checklist; its primary purpose is rather to identify the different deployment contexts and cross-cutting requirements that need to be taken into account when developing EPMwDC and likewise systems. This document provides an important contribution to the EPMwDC project and other likewise systems by linking cyber security engineering, regulatory compliance, data protection and defence-related information assurance requirements within a structured framework.

This report is intended to function as a living compliance document and should be updated periodically to reflect legislative changes, evolving cyber security and data protection obligations and developments affecting the EPMwDC project and likewise systems. Its scope is limited to regulatory and standards requirements, while other materials such as guidance, recommendations, case law, enforcement decisions, literature review and best practices are addressed separately.

1. EPMwDC Technical Specifications and Requirements

The EPMwDC system consists of several integrated hardware and software components designed to support the protection of sensitive information within controlled operational environments.

- The **preventative hardware component** is designed to interfere with unauthorised optical recording attempts by generating signals that reduce the ability of external imaging devices to capture readable visual information from protected displays or work areas. The module operates in a manner that does not interfere with normal human use of the protected environment while providing continuous protective coverage against certain forms of visual data acquisition.

- The **detection hardware component** is responsible for identifying potential recording or surveillance devices located within the monitored area. The module uses environmental sensing technologies and automated analysis mechanisms capable of distinguishing between ordinary environmental conditions and indicators associated with possible unauthorised monitoring activities. The system is designed to adapt to varying operational and environmental conditions in order to improve reliability and reduce false detections.

- The **software environment** coordinates the operation of the hardware components, processes sensor and monitoring data and supports the identification and management of potential security incidents. The software architecture includes functionalities relating to system control, event analysis, secure logging, encrypted data handling and dependency management. The system is also designed to support future scalability, maintainability, and integration with broader security management infrastructures.

- The **communications component** enables the secure transmission of system data, alerts and incident-related information to authorised external systems or remote monitoring environments. The module is intended to support protected communications, reliable information exchange and interoperability with centralised security or incident management platforms.

- The **remote server environment** provides centralised storage, analysis, and management functionalities for information received from deployed systems. It supports incident review, reporting, auditability, and controlled access to operational data while incorporating layered security measures intended to protect the confidentiality, integrity, and availability of stored and transmitted information.

2. Implementation Strategy

Understanding the phased implementation approach of the EPMwDC system is relevant for the purposes of regulatory and compliance analysis, as different legal, cyber security, data protection and operational requirements may apply at different stages of the system lifecycle.

The **initial phase** focuses on system integration, during which the hardware and software components are combined into a unified operational environment. This stage includes interoperability and compatibility testing to ensure that the various modules communicate effectively and can operate alongside existing digital infrastructure, monitoring systems and security management environments without disrupting operational continuity.

The **second phase** involves testing and validation activities intended to assess the overall effectiveness and reliability of the system under controlled conditions. Testing procedures may include simulated operational scenarios and controlled threat environments designed to evaluate the system's ability to detect potential unauthorised monitoring or recording activities, generate appropriate responses and maintain stable operation under varying environmental conditions. Validation activities also assess factors such as detection consistency, response efficiency, resilience and overall operational performance.

The **third phase** focuses on certification, assurance, and security evaluation processes intended to confirm that the system satisfies applicable technical, security and operational requirements prior to deployment. This stage includes reviews of system architecture, security mechanisms, operational safeguards and performance characteristics to assess the system's readiness for use within controlled or high-security operational environments.

Following successful evaluation, the **final phase** involves deployment and operational rollout within designated environments. Deployment activities include secure installation, configuration, system calibration, and operational verification, together with personnel training and familiarisation activities intended to ensure that authorised operators and security personnel are able to manage, monitor, and respond to system-generated events effectively.

3. Overview of the Relevant Regulatory Fields

The regulatory assessment of AI-enabled security and monitoring systems requires consideration of multiple overlapping legal and technical domains due to the complex interaction between AI, visual monitoring technologies, communications infrastructure and the handling of sensitive information.

One of the main regulatory domains concerns **cyber security** and information security requirements, including security by design. Systems intended to monitor sensitive environments or protect confidential information must address obligations relating to secure system architecture.

A further important domain relates to **personal data protection**. Even where a system is not designed to identify individuals directly, visual monitoring, image capture, metadata generation or alert transmission involve the processing of personal data. This raises legal considerations concerning lawful processing and implementation of safeguards intended to reduce unnecessary intrusions into individual privacy, especially considering privacy by design requirements.

Artificial intelligence governance and trustworthy **AI requirements** also represent a significant regulatory domain. AI-enabled monitoring systems may involve automated detection, classification, contextual analysis or decision-support functionalities that require additional assessment and implementation of supplementary measures.

In addition, **defence, national security and classified information** protection frameworks may become relevant where such technologies are deployed within governmental, military or other high-security operational settings.

The **dual-use** nature of advanced monitoring technologies further complicates the regulatory landscape. Systems capable of operating in both civilian and defence environments may simultaneously fall within multiple regulatory frameworks that differ in scope, terminology, operational expectations and compliance requirements. As a result, a comprehensive regulatory analysis requires an interdisciplinary approach capable of connecting technical system characteristics with legal, ethical, security and operational obligations across different domains and deployment contexts.

4. Regulatory Domains Relevant to the EPMwDC System

4.1. Methodological Scope of the Regulatory Mapping

The following regulatory analysis is structured around the system's functional characteristics rather than all potentially relevant requirements. For an EPMwDC-type system, the core relevant functions include visual monitoring of protected environments, AI-assisted detection of unauthorised capture attempts, preventative interference with optical recording, secure incident reporting, remote transmission and storage of alert data, audit logging, software maintenance, and deployment in civilian, governmental or defence-related settings.

The legal provisions referred to below are selected because they correspond most directly to the system's core technical and operational features. They are not intended to form an exhaustive list of all potentially applicable provisions. Where Lithuanian legislation is referred to below, this is done for illustrative purposes.

Other provisions of the same instruments referred to below, national implementing laws, sector-specific rules, etc. may also apply depending on the final system design, the end user, the deployment environment, the type of data processed and the classification level of the protected information.

4.2. Cybersecurity and Information Security

Cybersecurity regulation is relevant because an EPMwDC-type system is not merely a passive protective tool. It becomes part of the protected information environment. Its sensors, software and hardware components may all become attack surfaces. If compromised, the system could fail to detect an actual visual capture attempt, suppress or manipulate alerts, expose incident data, reveal protected screen content or provide an attacker with a path into a sensitive network. This means that the cybersecurity analysis must cover both the system's protective purpose and the security of the system itself. Below is provided the illustrative overview of the potentially applicable cybersecurity framework.

4.3. NIS2 Directive

The NIS2 Directive[1] is relevant where the system is deployed by, supplied to or integrated into an entity falling within an essential or important sector, such as public administration, healthcare, digital infrastructure, energy, transport or other regulated sectors. NIS2 establishes a cybersecurity framework for network and

[1] 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

information systems, with emphasis on governance, risk management, incident handling and supply chain security. The provisions below are highlighted because they are most directly relevant to the system's core cybersecurity risks, without excluding the possible relevance of other NIS2 requirements. The provider and deployer of the EPMwDC system should assess whether the NIS2 Directive applies to the relevant deployment context, in particular where the system is supplied to, integrated into, or operated by an essential or important entity. The provisions mentioned below are not exhaustive but are highlighted because they relate most closely to the system's cybersecurity governance.

Article 20 NIS2 requires Member States to ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken under Article 21 and oversee their implementation. It also provides that management bodies may be held liable for infringements. In practice, this means that decisions concerning the deployment of an EPMwDC-type system, including supplier selection, integration with existing infrastructure, accepted risk, training and incident escalation, should be addressed as part of the organisation's cybersecurity governance and not left solely to technical teams. Article 21 NIS2 is relevant because it requires essential and important entities to manage cybersecurity risks in a way that is appropriate to their systems and operations. For the EPMwDC system, this means assessing whether the device and its functions are sufficiently protected against foreseeable risks. The provision is also relevant because it covers the security of systems during acquisition, development and maintenance, including vulnerability handling and disclosure, which supports assessing the EPMwDC system from the design stage and throughout its lifecycle rather than only after deployment.

Article 23 NIS2 is relevant because it deals with reporting of significant incidents. A significant incident is one that has caused or is capable of causing severe operational disruption or financial loss for the entity concerned or has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. If the EPMwDC system is disabled, manipulated, compromised through its update mechanism, used to suppress alerts or exploited as a route into a protected network, the incident may need to be assessed under the applicable NIS2 notification framework.

NIS2 also reflects security-by-design requirements through Article 21(2)(e), which refers to security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure. For an EPMwDC-type system, this supports considering cybersecurity from the design stage and throughout the system lifecycle, including secure configuration, protected update mechanisms, vulnerability management and supplier-related security controls.

4.4. Cyber Resilience Act

The Cyber Resilience Act[2] is relevant where the system is placed on the EU market as a product with digital elements. It applies to connected hardware and software products and introduces cybersecurity requirements across the product lifecycle.

The most important concept for this system is security by design. Article 13 of the Cyber Resilience Act concerns manufacturer obligations relating to the design, development and production of products with digital elements. For the EPMwDC system, security by design means that protection against unauthorised access, secure default configurations, resilience against tampering, etc. should be part of the architecture from the beginning rather than added later as operational controls.

Article 14 of the Cyber Resilience Act is relevant because it concerns vulnerability and incident reporting obligations. An EPMwDC-type system may rely on operating system components, embedded software, third-party dependencies, etc. The system, therefore, requires a structured vulnerability-management process, including identification of affected components, remediation procedures and secure deployment of updates.

[2] 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 and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

The above articles are mentioned because they are the most relevant to the system's design, maintenance and security lifecycle, although other obligations under the Cyber Resilience Act may also apply depending on the final product configuration and deployment context.

4.5. Sector-specific cybersecurity rules

Sector-specific cybersecurity frameworks may become relevant depending on where the system is deployed. In the financial sector, Digital Operational Resilience Act (**DORA**)[3] establishes obligations concerning information and communications technologies (**ICT**) risk management, incident reporting, digital operational resilience testing and third-party ICT risk. If an EPMwDC-type system is used in a financial institution as part of its security or operational resilience framework, DORA-related requirements may influence procurement, ICT risk assessment, contractual controls and incident handling.

This illustrates why the system cannot be analysed only at product level but more detailed analyses need to be performed at a deployment level as well. The same technology may be subject to different cybersecurity expectations when deployed in a corporate boardroom, a hospital, a bank, a public authority, a classified research facility or a defence environment.

4.6. Data Protection and Privacy

Data protection law is relevant because an EPMwDC-type system may process visual images, video frames, behavioural indicators, device-related indicators, timestamps, location data, information about persons present in the monitored room and other personal data. Even where the system is not intended to identify individuals, visual and contextual information may still relate to identifiable persons and therefore constitute personal data under Article 4(1) of the General Data Protection Regulation (**GDPR**).[4]This is especially important because the system's alert package may be more sensitive than it first appears. It may reveal who was present, when the event occurred, where the monitor was located, what type of information was displayed or why the event was considered suspicious. The regulatory analysis must therefore cover not only image capture, but also alert generation and other related data processing operations.

Although all GDPR requirements may be relevant to the EPMwDC system, this section does not provide a full article-by-article GDPR assessment. Instead, it highlights selected provisions that best illustrate the main data protection issues raised by the system, while recognising that the remaining GDPR obligations must also be assessed as part of the broader compliance review before deployment.

4.7. GDPR applicability and core processing principles

Article 2(1) GDPR applies to wholly or partly automated processing of personal data. Since an EPMwDC-type system relies on automated monitoring, detection and reporting, GDPR applicability must be assessed whenever personal data are processed in a civilian or otherwise non-exempt context.

Article 5 GDPR is essential for all systems because it sets out the basic principles of processing which need to be complied with irrespective of the system development stage. Article 5(1) GDPR sets out the principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality, while Article 5(2) establishes the accountability principle.

- The principle of **lawfulness, fairness and transparency** means that the processing must have a valid legal basis, must not be used in a way that is unexpected or disproportionate, and must be

[3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, as available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[4] 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

communicated to individuals where required. For the EPMwDC system, this is relevant because persons present in a monitored room may be captured in incident-related data even if they are not the target of the monitoring. The controller should therefore be able to explain why the system is used, what data may be processed, who may access the data and how the monitoring is limited to the security purpose.

- The principle of **purpose limitation** requires the system to be used for clearly defined purposes, such as detecting and managing potential unauthorised visual capture of protected information. Data collected through the system should not later be reused for unrelated purposes, such as general employee performance monitoring, behavioural profiling or disciplinary analysis unrelated to the detected incident, unless a separate legal basis and purpose assessment support such use.
- The principle of **data minimisation** requires the system to process only the personal data that are necessary for its intended security function. For example, the system should not retain continuous footage of all persons present in a room if incident-based retention is sufficient. It should also avoid collecting information unrelated to the suspected unauthorised capture attempt, such as unnecessary details about bystanders or ordinary conduct that has no relevance to the incident.
- The principle of **accuracy** is relevant because inaccurate or misleading incident data may have consequences for individuals and for the security response. Alerts, timestamps and other data should therefore be reliable and sufficiently contextualised. If an alert is later found to be a false positive, the system records should allow this to be reflected so that incorrect assumptions are not preserved or acted upon.
- The principle of **storage limitation** requires personal data to be kept only for as long as necessary for the relevant purpose. For the EPMwDC system, this means that temporary video buffers, alert images, etc. should have defined retention periods. Data that are not linked to a relevant incident should generally not be retained, while incident-related data should be deleted or anonymised once they are no longer needed for verification, investigation, audit or other justified purposes.
- The principle of **integrity and confidentiality** requires appropriate protection against unauthorised or unlawful processing, accidental loss, destruction or damage. For the EPMwDC system, this is particularly important because incident packages may contain both personal data and sensitive operational information. Access controls, encryption and other technical and organisational measures are therefore necessary safeguards.
- Finally, the principle of **accountability** requires the controller to be able to demonstrate compliance with the GDPR principles. In practice, this means documenting the system's purpose, data flows, retention rules, access rights, security measures, DPIA findings where applicable, and the procedures for reviewing and escalating alerts. For the EPMwDC system, accountability is especially important because the system combines monitoring, automated analysis and security response in a way that must remain explainable and controlled.

4.8. Controller and processor roles under the GDPR

The GDPR qualification of the EPMwDC system manufacturer will depend on its actual role in the relevant processing activity. Under Article 4(7) GDPR, the manufacturer may act as a controller where it determines the purposes and means of processing, for example if incident data, diagnostic logs or performance information are used for its own purposes such as product improvement, model refinement or similar purposes.

More commonly, however, the system manufacturer is likely to act as a processor under Article 4(8) GDPR where it processes personal data on behalf of the deploying organisation, for example by hosting, maintaining or supporting the system according to the customer's instructions. In such cases, the relationship should be governed by a data processing agreement under Article 28 GDPR, while any independent use of data by the manufacturer would require a separate controller assessment, lawful basis under Article 6 GDPR and compliance with other GDPR provisions, applicable to controllers.

4.9. Lawful basis and deployment context

Article 6 GDPR requires a lawful basis for processing. The appropriate basis will depend on the controller, deployment setting and purpose of the system. A private company, a public authority, a financial institution, a hospital and a defence-related body may each require a different legal analysis.

Where the system processes special categories of personal data under Article 9 GDPR, such as biometric data used for the purpose of uniquely identifying a person, or other protected categories, an Article 6 lawful basis will not be sufficient on its own. In such cases, the controller must also identify a valid Article 9 condition and apply stricter safeguards. This may become relevant, for example, if the system is deployed in healthcare settings, captures health-related information, or is later configured to process biometric data for identification purposes.

This is methodologically important because it shows that the system does not have one fixed legal status. Its legal classification changes with the deployment context. The same technical function may be lawful under one configuration and disproportionate under another if the purpose, retention period, monitored population, safeguards or other deployment aspects differ.

4.10. Data subject rights and automated decision-making

Where the GDPR applies, the deployment of the EPMwDC system should also take into account data subject rights established in Chapter III of the GDPR. In practice, the scope and exercise of these rights will depend on the deployment context, the controller, the applicable legal basis and any lawful restrictions that may apply in sensitive security environments. Article 22 GDPR may also be relevant if system outputs are used for decisions producing legal or similarly significant effects for individuals; accordingly, alerts generated by the system should remain subject to meaningful human review rather than being treated as automatically determinative.

4.11. Privacy by design and by default

Article 25 GDPR requires the controller to implement appropriate technical and organisational measures both when determining the means of processing and during the processing itself, taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of processing, and the risks to the rights and freedoms of natural persons. These measures must be designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing. Article 25 further requires that, by default, only personal data necessary for each specific purpose are processed, including in relation to the amount of data collected, the extent of processing, the period of storage and data accessibility. Recital 78 similarly explains that controllers should adopt internal policies and implement measures meeting the principles of data protection by design and by default, including minimising processing, pseudonymising data as soon as possible, ensuring transparency, enabling data subjects to monitor processing and enabling the controller to create and improve security features.

For the EPMwDC system, this means that privacy safeguards should be considered already when the monitoring, detection, alerting and reporting functions are designed, not only after deployment. For example, data protection by design may support an architecture in which temporary video buffers are overwritten unless a defined incident threshold is met, only incident-specific data are preserved, and any retained information is limited to what is necessary for verification, escalation and response. These are examples rather than a closed list of measures.

Data protection by default is also relevant to the system's ordinary configuration. By default, the system should not retain more visual or contextual data than necessary, should not make incident records broadly accessible, and should not permit wider use of alert data for unrelated purposes. Depending on the final deployment context, appropriate safeguards may include local processing where feasible, masking or minimisation of bystander data, role-based access controls, encryption of incident packages, defined retention periods, separation of incident records from unrelated personnel files and documented review

procedures. The precise measures should be determined through the broader data protection assessment, taking into account the monitored environment, the categories of data subjects, the sensitivity of the information involved and the risks created by the intended processing.

4.12. Security of processing and incident data protection

Article 32 GDPR requires appropriate security of processing, including, among others, measures that address confidentiality, integrity, availability and resilience. For this system, Article 32 overlaps with cybersecurity regulation, but its purpose is specifically to protect personal data processed by the system. This means that implemented security measures are not merely technical best practices. They are part of the data protection compliance model.

4.13. Data Protection Impact Assessment

Article 35 GDPR may require a Data Protection Impact Assessment (**DPIA**) where the processing is likely to result in a high risk to the rights and freedoms of natural persons. This is particularly relevant for systems such as EPMwDC, where monitoring and automated analysis may take place in environments in which individuals have limited control over the processing and the information involved may be sensitive.

For the EPMwDC system, the DPIA, among others, should examine whether the intended processing is necessary and proportionate, what risks it may create for data subjects and what measures are needed to address those risks. At the development stage, this assessment can already inform key design choices, such as limiting unnecessary data capture, securing incident records and ensuring meaningful human review. However, a final DPIA can only be completed once the actual deployment context is clear, including the controller, purpose of use, monitored environment, categories of data subjects and operational safeguards.

4.14. Law Enforcement Directive and national security processing

Where the system is used by competent authorities for law enforcement purposes, the Law Enforcement Directive[5] may apply instead of the GDPR. The Directive governs personal data processing by competent authorities for the prevention, investigation, detection or prosecution of criminal offences and related public-security purposes.

Where the system is used for national security or defence purposes, national legal frameworks may apply because national security remains primarily within Member State competence. This is also reflected in Article 2(2)(a) GDPR, which excludes processing carried out in the course of activities falling outside the scope of the EU law, and Article 2(2)(b) GDPR, which excludes processing by Member States when carrying out activities falling within the scope of the Common Foreign and Security Policy. This distinction is important because the same technical system may be subject to GDPR in a corporate setting, the Law Enforcement Directive in a law enforcement setting and national security or defence-specific rules in a military or intelligence setting.

4.15. Artificial Intelligence Regulation

AI regulation is relevant because an EPMwDC-type system uses AI system to detect indicators of unauthorised visual capture. The key legal issue is not merely that AI is used. The more important question is how AI outputs affect operational decisions.

[5] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, as available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng.

A false positive may wrongly characterise ordinary conduct as suspicious. A false negative may allow protected information to be captured. The AI component therefore has legal significance because it influences the reliability, proportionality and accountability of the system.

4.16. AI Act scope and military, defence and national security exclusion

The AI Act[6] establishes harmonised rules for AI systems placed on the market, put into service or used in the EU. Article 2 defines the scope of the AI Act while Article 2(3) is particularly important for dual-use systems because the AI Act excludes AI systems placed on the market, put into service or used exclusively for military, defence or national security purposes.

The word "exclusively" is essential. Where the same system is developed, marketed or supplied for both civilian and defence settings, the exclusion should not be assumed for all use cases. An EPMwDC-type system used in a corporate boardroom, public authority, healthcare facility or financial institution may still require AI Act analysis even if similar functionality is also used in defence environments.

4.17. Risk classification

The system's classification under the AI Act depends on its intended purpose, technical configuration and deployment context. The AI Act follows a risk-based model, distinguishing between prohibited AI practices, high-risk systems, systems subject to specific transparency obligations and minimal-risk systems.

An EPMwDC-type system used only as a narrow security tool to detect unauthorised visual capture may fall outside the higher-risk categories, but this may change if it is used for law enforcement support, employment-related monitoring, access control, biometric functions, critical infrastructure protection or other contexts listed in the AI Act.

Depending on the applicable risk level, different obligations apply under the AI Act, ranging from prohibition of certain AI practices to transparency duties or more extensive compliance requirements for high-risk systems. The following section therefore focuses on selected main obligations for high-risk AI systems, as these are the obligations most likely to influence the design, development, etc. of an EPMwDC-type system where its use or context brings it within the high-risk category.

4.18. Risk management, governance, oversight and system reliability

Where the EPMwDC system falls within the high-risk AI framework, Article 9 AI Act requires a "risk management system" to be "established, implemented, documented and maintained" as a "continuous iterative process" throughout the system lifecycle. For EPMwDC, this means identifying and managing risks linked to its intended purpose and reasonably foreseeable misuse, including incorrect alerts, missed detections and operational misuse of the detection function.

Article 10 requires data governance and management practices that are appropriate for the system's intended purpose. In the EPMwDC context, this means that training, validation and testing data should be relevant and sufficiently representative of the environments in which the system is expected to operate, such as different rooms, lighting conditions, screens, reflective surfaces and recording-device scenarios.

Articles 11 and 12 require technical documentation and record-keeping. For EPMwDC, this supports documenting the system's intended purpose, performance, limitations, risk controls and testing, as well as maintaining logs that allow relevant detections, outputs and operator review to be traced.

Articles 13 and 14 require transparency and human oversight. Deployers should be able to interpret the system's output and use it appropriately, while authorised personnel should be able to review, disregard, override or reverse outputs where appropriate. For EPMwDC, this means that alerts should support human assessment rather than automatically determine escalation.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), as available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

Article 15 requires an appropriate level of accuracy, robustness and cybersecurity throughout the system lifecycle. For EPMwDC, this supports testing the system against realistic operating conditions and foreseeable attempts to interfere with or manipulate detection performance.

Finally, the system documentation should clearly distinguish object-based or behavioural detection from biometric identification, biometric categorisation or emotion recognition, if those functions are not part of the EPMwDC system.

4.19. Defence, National Security, Classified Information and Dual-Use Controls

4.20. Regulatory relevance of defence and classified-information contexts

This domain is relevant because the system is intended to protect confidential or classified information from unauthorised visual capture. The same system may be used in corporate boardrooms, government offices, financial institutions, healthcare facilities, research centres, military briefing rooms or NATO-related facilities. Its legal classification therefore depends on context: the end user, deployment location, information classification level, connectivity model, export destination and operational purpose.

4.21. EU Dual-Use Regulation

The EU Dual-Use Regulation[7] establishes the EU regime for export controls, brokering, technical assistance, transit and transfer of dual-use items. Article 2(1) of the regulation defines dual-use items as items, including software and technology, that can be used for both civil and military purposes. Article 3 establishes authorisation requirements for listed dual-use items, while Article 4 may become relevant in certain sensitive end-use situations.

For an EPMwDC-type system, this does not mean that the system is automatically controlled. It means that classification and end-use assessment are necessary. The analysis should consider whether the hardware, software, or other system components fall within controlled categories, particularly where transfer outside the EU is involved.

4.22. Classified information and EU security rules

Where the system is deployed in environments handling EU classified information, Council Decision 2013/488/EU[8] on the security rules for protecting EU classified information may become relevant. The Decision establishes a framework for protecting EU classified information, including but not limited to information assurance, personnel security, physical security and protection of classified information in communication and information systems.

For the system, the key point is that incident data may itself become sensitive or classified. An alert package may reveal what was displayed on the protected screen, where the meeting occurred, who was present and when the event took place. The system's outputs should therefore be analysed as potentially protected information, not merely as ordinary technical logs.

4.23. NATO security and information assurance

For NATO-related deployments, the system must be assessed with caution. NATO security and information assurance requirements may become relevant where NATO classified information is handled or where the system is connected to NATO communication and information systems. Publicly available NATO materials set out general principles for protecting NATO classified information, including safeguarding confidentiality,

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

[8] 2013/488/EU: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, as available at: https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng.

integrity and availability.[9] They also support a high-level assessment of areas such as access control, physical security, communication and information system security, industrial security, classified-information handling and the protection of information systems.

However, this public material cannot provide a complete basis for deployment in a NATO environment. Many NATO security, accreditation and information assurance requirements are classified or otherwise not publicly available. As a result, any deployment of the system in a NATO-related context would require additional classified assessments by appropriately authorised personnel. The system's preventative, detective and reporting functions may be relevant to NATO security objectives, particularly where they help prevent unauthorised disclosure of classified information through visual capture. Nevertheless, its suitability for NATO use cannot be confirmed solely based on public sources.

4.24. Cumulative nature of civilian and defence obligations

Defence or national-security use does not automatically remove civilian legal obligations in all circumstances. The EU legislation contain certain exclusions for certain military, defence, national-security or classified-information contexts but those exclusions must be assessed carefully and by reference to actual use. A system developed by a private provider and supplied across both civilian and defence markets may remain subject to EU regulatory obligations for non-exempt uses.

This cumulative structure is one of the most important findings for the regulatory analysis. The system may need to satisfy product cybersecurity requirements, data protection obligations, AI governance rules, export-control assessments and defence accreditation expectations at the same time, depending on deployment.

5. Cross-cutting insihts and conclusions

While every separate aspect of the applicable regulatory component is important, there are certain regulatory cross-cutting aspects which must be considered throughout the cycle of the EPMwDC system.

5.1. Lifecycle-based compliance

Overall, the regulatory assessment should not be treated as a one-off exercise carried out only before deployment. For an EPMwDC-type system, compliance has to be considered throughout the full lifecycle of the system, from design, development, training and testing to integration, operation, maintenance, updates and eventual decommissioning. This is because different obligations become particularly important at different stages (without undermining their importance in other stages): security by design and privacy by design shape the initial architecture, AI risk management and data governance inform development and testing, logging, human oversight and incident handling are central during operation, and vulnerability management, secure updates remain relevant for as long as the system is supported.

5.2. Generated incident data as a regulated object

A further conclusion is that the system should not be viewed only as a tool for protecting sensitive information. In performing that function, it may also generate new information that is itself legally sensitive. Alerts, logs, confidence scores, captured images, timestamps, room identifiers and references to screen content may, depending on the context, amount to personal data, confidential information or classified

[9] See for example: NATO Security Policy, C-M(2002)49, "Security within the North Atlantic Treaty Organisation (NATO)", as available at: https://archives.nato.int/uploads/r/nato-archives-online/6/9/2/692d2a4b1ed8484535e036b018137165b415473cb83a9e248e51e477a021f4e5/C-M_2002_49_INCLUDING_COR1_TO_COR11_ENG_NHQP1863340.pdf?.

information. For this reason, the reporting and storage functions should be treated as part of the regulated system, rather than as merely technical or administrative components.

5.3. Human oversight as a connecting requirement

Human oversight is another cross-cutting element of the regulatory analysis. It helps ensure that alerts are not treated as automatic conclusions but are reviewed in light of the surrounding context before any action is taken. For an EPMwDC-type system, this is particularly important where an alert may relate to identifiable individuals or lead to a security response. Embedding human review into the incident-response process supports proportionality, accountability and a more balanced use of automated detection.

Bibliography

1. GDPR. European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation, as available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
2. Law Enforcement Directive. European Parliament and Council. (2016). Directive (EU) 2016/680 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 by competent authorities, as available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng.
3. NIS2 Directive. European Parliament and Council. (2022). 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, as available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.
4. DORA. European Parliament and Council. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, as available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.
5. AI Act. European Parliament and Council. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, as available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
6. Cyber Resilience Act. European Parliament and Council. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, as available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.
7. Cybersecurity Act. European Parliament and Council. (2019). Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification, as available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.
8. Dual-Use Regulation. European Parliament and Council. (2021). Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, as available at: https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng.
9. Council Decision on EU Classified Information. Council of the European Union. (2013). Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information, as available at: https://eur-lex.europa.eu/eli/dec/2013/488/oj/eng.
10. Charter of Fundamental Rights of the European Union. European Union. (2012). Charter of Fundamental Rights of the European Union, as available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT.
11. European Convention on Human Rights. Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms, as available at: https://www.echr.coe.int/european-convention-on-human-rights.
12. Geneva Conventions. International Committee of the Red Cross. (1949). The Geneva Conventions of 1949 and their Additional Protocols, as available at: https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries.
13. NATO Security Policy. North Atlantic Treaty Organization. Security within the North Atlantic Treaty Organisation, C-M(2002)49, including corrigenda, as available at: https://archives.nato.int/uploads/r/nato-archives-online/6/9/2/692d2a4b1ed8484535e036b018137165b415473cb83a9e248e51e477a021f4e5/C-M_2002_49_INCLUDING_COR1_TO_COR11_ENG_NHQP1863340.pdf.
14. NATO Security Policy. North Atlantic Treaty Organization. Security within the North Atlantic Treaty Organisation, C-M(2002)49, publicly available copy, as available at: https://www.gns.gov.pt/docs/cm-2002.pdf.
15. NATO Management of Non-Classified Information Policy. North Atlantic Treaty Organization. Policy on Management of Non-Classified NATO Information, C-M(2002)60, as available

at: https://www.nato.int/content/dam/nato/webready/documents/Archives/policies/Management-non-classified-information-en.pdf.

16. NATO Personal Data Protection Framework. North Atlantic Treaty Organization. NATO Personal Data Protection Framework, as available at: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/20240901_NATO-personal-data-protection-f.pdf.
17. NATO ACT Personal Information and Privacy Protection Directive. Allied Command Transformation. Personal Information and Privacy Protection Directive, as available at: https://www.act.nato.int/wp-content/uploads/2023/05/rfi022059-privacy-directive.pdf.
18. NATO Information Assurance. North Atlantic Treaty Organization. NATO Information Assurance resources, as available at: https://www.ia.nato.int.
19. NATO Cyber Defence. North Atlantic Treaty Organization. Cyber Defence topic page, as available at: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence.
20. NATO Cyber Defence Resources. NATO Multimedia Library. Cyber Defence resources, as available at: https://natolibguides.info/cyberdefence.
21. NATO Cyber Defence Pledge. North Atlantic Treaty Organization. Cyber Defence Pledge, 8 July 2016, as available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge.
22. NATO Artificial Intelligence Strategy. North Atlantic Treaty Organization. Summary of the NATO Artificial Intelligence Strategy, 22 October 2021, as available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy.
23. NATO Revised Artificial Intelligence Strategy. North Atlantic Treaty Organization. Summary of NATO's Revised Artificial Intelligence Strategy, 10 July 2024, as available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.
24. Cyber Resilience Act. European Commission. Cyber Resilience Act policy page, as available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.
25. Cyber Resilience Act Implementation. European Commission. Cyber Resilience Act implementation page, as available at: https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation.
26. NIS2 Directive. European Commission. NIS2 Directive policy page, as available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.
27. Dual-Use Export Controls. European Commission. Exporting dual-use items, as available at: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.
28. EU Classified Information. Council of the European Union. Council security rules for protecting classified information, summary page, as available at: https://eur-lex.europa.eu/EN/legal-content/summary/council-security-rules-for-protecting-classified-information-euci.html.
29. EU Policy on Cyber Defence. European External Action Service and European Commission. Joint Communication on the EU Policy on Cyber Defence, as available at: https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.