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: ***HIPSTER***

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

Action result: ***Modeling According to the Principles of Privacy by Design and Privacy by Default: Architectural Requirements***

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

Table of Contents

Introduction

The project "Hybrid, Information, Psychological, Societal Threats handling system for public security domain practitioners, businesses, and education" - HIPSTer aims to create a comprehensive solution for handling hybrid, information, psychological, and societal threats for the public security domain and businesses.

The HIPSTer project aims to develop and an advanced software solution – a Hybrid Information Psychological Societal Threats Handling System that utilizes recent advancements in OSINT, SocMINT, NLP, and AI to automatically detect, attribute, and counter or prevent prioritized threats, including hybrid threats.

To successfully embed the principles of "Privacy by Design" (PbD) and "Security by Design" (SbD) into a system, its foundational architecture must be engineered to comply with regulatory frameworks, such as the GDPR, EU AI Act, Cyber Resilience Act.

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

1. Project Context and Regulatory Scope

The Hybrid Information Psychological Societal Threats Handling System (HIPSTer) is a critical technological infrastructure designed to automate the detection, attribution, and prevention of hybrid, psychological, and societal threats. By integrating Open-Source Intelligence (OSINT), Social Media Intelligence (SocMINT), Natural Language Processing (NLP), and AI-driven analytics, the system provides a 24/7 monitoring capability for public security practitioners and essential entities.

The architectural integrity of HIPSTer is governed by an interconnected "Digital Rulebook." Architectural controls must enforce compliance with:

- **EU General Data Protection Regulation (GDPR):** Regulation (EU) 2016/679.
- **EU AI Act:** Regulation (EU) 2024/1689.
- **NIS2 Directive:** Directive (EU) 2022/2555 (transposed via the 2024 Lithuanian Law on Cyber Security).
- **Lithuanian Law on Legal Protection of Personal Data (ADTAI):** Including 2024 amendments.
- **Law Enforcement Directive (LED):** Directive (EU) 2016/680.

The system performs four primary categories of personal data processing, each requiring specific technical safeguards:

1. **OSINT and SocMINT Collection:** Automated gathering of identifiers and behavioral content from public domains.
2. **AI-driven Profiling and Behavioral Analysis:** Detection of coordinated manipulation and extremist patterns.
3. **Threat-Intelligence Sharing:** Secure exchange of analytical indicators between consortium stakeholders.
4. **Training Dataset Creation:** Processing data for machine-learning model development and bias mitigation.

2. Core Principles: Privacy by Design (PbD) and Privacy by Default

In strict accordance with Article 25 GDPR, the architecture must treat data protection as a fundamental technical requirement rather than a post-development add-on.

Privacy by Design

Privacy must be embedded throughout the development lifecycle. Architectural controls must enforce:

- **Purpose-Specific Data Flows:** Data must be technically siloed, accessible only to modules with a verified threat-detection requirement.
- **Lifecycle Integrity:** Data protection measures must be active from initial ingestion through to disposal, ensuring no "security gaps" exist during state transitions.
- **Automated Risk Mitigation:** Integration of Data Protection Impact Assessments (DPIAs) directly into the deployment pipeline to evaluate risks to democratic trust and fundamental rights.

Privacy by Default

The system must automatically enforce the most restrictive privacy settings.

- **Collection Limitation:** Ingestion filters must be configured to discard any metadata or content that does not match prioritized threat indicators.
- **Storage Limitation:** Failure to implement automated, purpose-linked retention enforcement triggers significant legal liability for non-material damage (C-200/23).
- **Default Anonymization:** AI models must operate on the principle of minimal processing, filtering out non-essential identifiers at the collection layer.

3. High-Risk AI System Requirements (EU AI Act Compliance)

HIPSTer is classified as a "High-Risk AI System" under Annex III of the EU AI Act due to its use in public security and law enforcement contexts.

AI Act Compliance for High-Risk Architecture

Requirement	Description	Architectural Implementation
Risk Management (Art. 9)	Continuous, documented lifecycle risk system.	Centralized risk register; iterative red-teaming; mitigation of fundamental rights risks.
Data Governance (Art. 10)	Datasets must be relevant, representative, and bias-audited.	Dataset audits; provenance tracking; processing of sensitive data solely for bias correction (Art. 10 exception).
Technical Documentation (Art. 11)	Detailed documentation of architecture and logic.	Auto-generated model cards; version-controlled data lineage; system logs.
Transparency (Art. 13)	Enabling users to interpret outputs and logic.	Explainability dashboards providing SHAP/LIME rationales for risk scores.

Human Oversight (Art. 14)	Mandatory human intervention and override capability.	"Human-in-the-loop" as the default; mandatory review for high-impact escalations.

Note on National Security Exemption: Architectural modes used *exclusively* for national security purposes by competent authorities fall outside the AI Act scope per Art. 2(3). However, "dual-use" modes remain strictly subject to these requirements.

Human-in-the-loop (HITL) Requirement

The architecture must prevent autonomous consequential actions. Any high-impact decision—such as law enforcement escalation or long-term blocking recommendations—must be subject to mandatory human validation.

4. Architectural Layer Compliance Mapping

4.1. Data Collection Layer

- **Metadata Provenance Tracking:** Every ingested data point must be tagged with its source, timestamp, and legal-basis (e.g., Art. 6(1)(e) for public task).
- **Regime Segregation:** The architecture must enforce a technical "hard wall" between GDPR-governed data and LED-governed law enforcement streams. Mixing these datasets constitutes a major compliance failure.

4.2. Data Processing Layer

- **Fact vs. Assessment Tagging:** Per Art. 7 LED, the system must distinguish between factual personal data and AI-generated assessments (intelligence inferences).
- **Pseudonymization Standards:** Following *EDPS v SRB* (C-413/23 P), the system must treat pseudonymized data as personal if the controller has the means to re-identify it. False security assumptions regarding "anonymized" data must be avoided.
- **Automated Retention:** The layer must execute purpose-specific erasure once threat research or investigation windows close.

4.3. AI/Analytics Layer (XAI)

- **Explainable Logic:** Per CJEU C-203/22 (*Dun & Bradstreet*), the system cannot unilaterally deny access to its logic by claiming trade secrets. The architecture must allow the submission of logic parameters to a supervisory authority for balancing rights against commercial protections.
- **Logic Transparency:** The system must provide "meaningful information about the logic involved" (e.g., data weighting) to satisfy the data subject's right of access.

4.4. Decision & Response Layer

- **Operational Benchmarks:** Integration with the Lithuanian **Strategic Communication Coordination Group** for real-time situational awareness.
- **Auditability:** All decisions must be traceable. Failure to document detections violates the state's obligation to investigate credible reports (*Beizaras and Levickas v. Lithuania*).

5. Key Implementation Stages for Compliance

1. **Socio-Technical Design & Risk Assessment:** Evaluating threats as psychological/societal harms and conducting initial DPIAs to prevent chilling effects on expression.
2. **Data Preparation and Bias Mitigation:** Managing the "regulatory complexity" where AI Act Art. 10 allows sensitive data processing for bias correction, despite GDPR Art. 9 restrictions.
3. **Adversarial Testing (Red-Teaming):** Proactive testing against "data poisoning," model manipulation, and jailbreak attempts.
4. **Operational Monitoring & Human Oversight:** Continuous tracking of false positives and enforcing intervention protocols.

Architectural Warning: The "Implementation Lag." Per Kilian R, et al. (2025), technical standards are emerging less than 6 months before enforcement. Architects must design for flexibility to accommodate shifting harmonized standards without requiring a total system redesign.

6. Technical Security and Data Integrity Measures

HIPSTer must implement security-by-design to meet GDPR Art. 32 and NIS2 requirements, leveraging **ENISA's Multilayer Framework**.

Security and Compliance Specifications

Security Measure	Requirement Source	Technical Specification
Encryption	GDPR Art. 32, NIS2	AES-256 (at rest); TLS 1.3 (in transit). Key management via EU-region HSM.
Access Control	GDPR, NIS2, LED	RBAC and MFA for all accounts; session recording for high-privilege access.
Data Integrity	NIS2, AI Act Art. 15	Safeguards against "model inversion" and poisoning; adversarial robustness.
LED Logging	LED Art. 25	Tamper-evident logs (hash-chaining) for **collection, consultation, disclosure, and erasure**.

Liability Risk: Architects are cautioned that a "loss of control" over data for even a limited period constitutes non-material damage (CJEU C-200/23), mandating zero-tolerance for unlogged data movements.

7. ELSA (Ethical, Legal, and Social) Architectural Constraints

The following non-negotiable constraints must be integrated into the system logic:

- **Contextual Disambiguation:** AI models must distinguish satire, journalism, and academic debate from hate speech to protect Art. 11 CFR rights.
- **Media Protection Thresholds:** Automatically lowered sensitivity for recognized media outlets to prevent over-blocking.
- **Traceability for Justice:** All detections provided to authorities must be documented to satisfy the state's obligation to investigate reports (*Beizaras and Levickas v. Lithuania*).

- **Prohibited Practices Monitoring:** Automated alerts to prevent "Subliminal Techniques" or "Manipulative Practices" prohibited under Art. 5 AI Act.

8. Final Architecture Compliance Checklist

Data Protection (GDPR/ADTAI/LED)

- [ ] **Art. 25 GDPR:** Privacy by Design and Default verified in all modules.
- [ ] **Art. 35 GDPR:** DPIA completed, specifically addressing the risk of non-material damage from loss of control (C-200/23).
- [ ] **Art. 15(1)(h) GDPR:** Interface allows access to logic/weighting (per C-203/22 balancing test).
- [ ] **Art. 7 LED:** Technical tagging distinguishing between factual data and assessments.
- [ ] **Art. 25 LED:** Hash-chained logs for collection, consultation, disclosure, and erasure.

AI Ethics (AI Act)

- [ ] **Art. 5 AI Act:** Verification that no manipulative or subliminal techniques are present.
- [ ] **Art. 10 AI Act:** Bias mitigation protocols established using sensitive data exceptions.
- [ ] **Art. 14 AI Act:** "Human-in-the-loop" override mechanism integrated for law enforcement.
- [ ] **Art. 27 AI Act:** Fundamental Rights Impact Assessment (FRIA) conducted for public body deployment.
- [ ] **Art. 50 AI Act:** AI-generated reports and counter-narratives clearly labeled as AI-content.

Cybersecurity (NIS2/CRA)

- [ ] **Art. 21 NIS2:** Documented policies for incident handling and secure development.
- [ ] **Art. 23 NIS2:** Early warning (24h) and detailed notification (72h) workflows integrated with NCSC.
- [ ] **Art. 15 AI Act:** Adversarial robustness and data/model poisoning defenses verified.
- [ ] **ENISA Framework:** Alignment with the Multilayer Framework for AI Security.
- [ ] **Lithuanian Operational Benchmarks:** System tested in "Cyber Shield OpEx" or equivalent exercises.

Annex: Implementation Framework, Compliance Checklists, and Architectural Challenges for the HIPSTer System

This framework defines the mandatory architectural requirements, regulatory benchmarks, and operational safeguards for the Hybrid Information Psychological Societal Threats Handling System (HIPSTer). As a system designed to counter Foreign Information Manipulation and Interference (FIMI) and multi-domain hybrid threats, its deployment must satisfy the stringent "Digital Rulebook" of the European Union while maintaining tactical efficacy.

1. Phased Architecture and Implementation Lifecycle

The HIPSTer system's trajectory from design to autonomous operation is governed by a four-stage lifecycle that synchronizes technical maturity with socio-technical risk management.

Stage 1: Socio-Technical Design & Risk Assessment

- **Objective:** Mandate the evaluation of threats as complex social and psychological harms, transcending traditional IT failure models.
- **Practical Steps:**
  - Construct comprehensive "psychological profiles" of adversaries, auditing for **means, motives, and opportunities** to exploit societal vulnerabilities.
  - Conduct a baseline assessment of the tool's impact on democratic trust and fundamental rights prior to technical hardening.
  - Define the "socio-technical" defense perimeter, accounting for human cognitive biases and the potential for "Fear, Uncertainty, and Doubt" (FUD) campaigns.

Stage 2: Data Preparation & Ethics

- **Objective:** Navigate the Threat Intelligence Maturity Model (Reactive → Proactive → Predictive → Autonomous) while resolving the tension between aggressive OSINT/SocMINT collection and data protection.
- **Practical Steps:**
  - Operationalize data normalization to fuse disparate Publicly Available Information (PAI) and Commercially Available Information (CAI) into meaningful ontologies.
  - Invoke AI Act Art. 10(5) protocols to permit processing of special category data (e.g., political opinions) strictly for bias monitoring and correction.
  - Establish strict purpose-limitation filters to ensure OSINT ingestion complies with the latest European Data Protection Board (EDPB) guidance on publicly accessible personal data.

Stage 3: Adversarial Testing

- **Objective:** Proactively stress-test the system against malicious manipulation and cyber-offensive techniques.
- **Practical Steps:**
  - Mandate "red-teaming" exercises specifically targeting **jailbreak attempts** and **model inversion** to protect system logic.
  - Simulate "data and model poisoning" attacks to verify the resilience of the threat intelligence graph against corrupted training inputs.
  - Utilize National Regulatory Sandboxes to validate technical compliance with emerging harmonized standards before full-scale deployment.

Stage 4: Operational Monitoring & Communication

- **Objective:** Maintain 24/7 situational awareness and autonomous detection while operationalizing reputation management.
- **Practical Steps:**
  - Deploy automated Natural Language Processing (NLP) to detect AI-supported social engineering, which currently accounts for over 80% of observed incidents.
  - Execute technical drills modeled on Lithuania's "Cyber Shield OpEx," integrating public communication teams to manage media responses during disinformation events.
  - Monitor for "narrative shifts" and coordinated inauthentic behavior (CIB) to provide real-time attribution of hybrid campaigns.

2. Multi-Layered Regulatory Compliance Checklists

Table 1: AI Act Requirements for High-Risk Systems

Requirement	Description	HIPSTer-Specific Measures
Risk Management (Art. 9)	Continuous, documented cycle throughout the AI life cycle.	Centralized risk register; iterative red-teaming for privacy, bias, and fundamental rights.
Data Governance (Art. 10)	Datasets must be relevant, representative, and bias-audited.	Dataset scans for sensitive attributes; strict exclusion of bias except where strictly necessary for correction.
Technical Documentation (Art. 11)	Detailed architecture, training, and performance records.	**Auto-generated model cards** and automated data lineage tracking for regulatory audit.
Transparency (Art. 13)	Users must be able to interpret system logic and limitations.	Explainability dashboards providing scoring rationales and uncertainty estimates for threat flags.
Human Oversight (Art. 14)	System must allow for effective human intervention/override.	Mandatory Human-in-the-loop (HITL) for all high-impact actions (e.g., reporting to LEAs).
Accuracy & Robustness (Art. 15)	Resilience against data poisoning and adversarial attacks.	Model drift detection; adversarial robustness testing; integration with SOC/SIEM telemetry.
Fundamental Rights (Art. 27)	Assessment of impact on privacy, expression, and democracy.	Mandatory Fundamental Rights Impact Assessment (FRIA) covering potential chilling effects.
Post-Market Monitoring (Art. 61)	Ongoing performance tracking after deployment.	**Automated telemetry** and quarterly AI safety reports documenting false-positive/negative rates.

Table 2: GDPR & Lithuanian ADTAI Alignment

Provision	Description	Updated Compliance Measures

Privacy by Design (Art. 25)	Integration of protection into design and default settings.	End-to-end encryption; automated data minimization for OSINT collection; purpose-specific flows.
DPIA (Art. 35)	Assessment for high-risk monitoring and profiling.	Updated assessments triggered by model changes; integration of Lithuanian 2024 public-sector transparency rules.
Data Subject Rights (Art. 12-23)	Mechanisms for access, rectification, and erasure.	Interfaces to manage requests; incorporation of the **video surveillance pre-complaint procedure** (ADTAI 2024).
Supervisory Oversight	SDPI expanded mandate under 2024 Lithuanian amendments.	Technical hooks for SDPI audit of **AI-supported high-risk data analytics** and algorithmic processing.

Table 3: Specialized Regulations (NIS2, DSA, & Criminal Code)

Regulation	Requirement	HIPSTer Implementation Measure
NIS2 (Art. 21/23)	Risk Management & Reporting	24h early warning; 72h incident notification; 30-day final report capability for digital infrastructure.
DSA (Art. 14)	**Trusted Flagger** Status	Ensure all generated notices are **precise and substantiated**, providing "logical weighting" to support platform action.
DSA (Art. 24)	Content Labeling	Clear marking of AI-generated counter-measures and reports to prevent inadvertent disinformation spread.
Lithuanian Criminal Code (Art. 170)	Incitement to Hatred	Context-aware NLP to distinguish criminal incitement from satire/political speech (per **SC Case 2K-86-648/2016**).

3. Practical Implementation Challenges

1. **The *Schufa* Impact on Scoring (C-634/21):** The CJEU ruling mandates that generating probability values (scoring) constitutes "automated individual decision-making" if a third party relies on them significantly. HIPSTer must architect for strict transparency and human intervention, as its threat scores will be viewed by regulators through this expanded legal lens.
2. **Transparency vs. Security (The Trade Secret Trap):** Per *Dun & Bradstreet* (C-203/22), the agency cannot use trade secrets to flatly refuse disclosure of system logic. Architects must provide the **logic and weighting** of data to the **supervisory authority** for balancing, ensuring transparency without handing adversaries a roadmap for model poisoning.
3. **Loss of Control Liability (C-200/23):** The ruling in *Agentsia po vpisvaniyata* establishes that "loss of control" over personal data for even a "limited period" constitutes non-material damage. This significantly lowers the threshold for litigation, necessitating bulletproof data integrity and immediate containment protocols.
4. **The "Subliminal" vs. "Persuasion" Gap:** The AI Act prohibits techniques that distort behavior. There is a critical legal friction point in distinguishing "lawful persuasion" (counter-narratives) from "prohibited manipulation." System designers must establish precise architectural thresholds to ensure automated responses do not impair informed decision-making.
5. **Implementation Lag & Dispersed Enforcement:** With a technical standard implementation window often falling below 6 months against a realistic 12-month requirement, the system faces the risk of

"dispersed enforcement"—where compliance in Lithuania may not satisfy the specific interpretations of authorities in France or Germany.

4. Technical Mitigation Strategies and System Safeguards

- **Data Integrity & Poisoning Defense:**
  - Operationalize **adversarial robustness testing** to identify vulnerabilities in the threat intelligence graph.
  - Deploy **model drift detection** to ensure that adversarial "data/model poisoning" does not cause the AI to deviate from its safety-aligned training parameters.
- **Security Controls:**
  - **Encryption:** Mandatory AES-256 for data at rest and TLS 1.3 for data in transit.
  - **Authentication:** Multi-Factor Authentication (MFA) for all administrative and operational access.
  - **Access Control:** Employ **Attribute-Based Access Control (ABAC)** for LED-mode processing and **Role-Based Access Control (RBAC)** for civilian/research streams to ensure strict legal segregation.
- **Auditing and Separation of Concerns:**
  - **Tamper-Evident Logging:** Implement **write-once logs** using **hash-chaining** and timestamping to satisfy LED (Law Enforcement Directive) requirements for a permanent, untamperable audit trail.
  - **Differentiated Operational Modes:** Technically segregate data streams governed by GDPR, LED, and National Security exemptions to prevent unlawful data mixing.
- **Human-in-the-loop (HITL) Workflows:**
  - Mandate human review for "content-context disambiguation" (satire vs. incitement) to comply with Lithuanian Supreme Court case-law (2K-86-648/2016).
  - Default HITL protocols for all legally significant decisions, such as escalation to law enforcement or long-term account blocking.

5. Comparative Best Practices for Hybrid Threat Architecture

Comparative Insights

Feature	Implementation Insight (Source: SOTA Analysis)
Ontology Creation	Transform raw data into "meaningful objects" (people, events) to reduce data noise and prevent "death by data" (Palantir Insight).
Intelligence Graph	Index 1 million+ sources to contextualize threats and facilitate the transition from Reactive to **Autonomous** operations (Recorded Future Insight).
Visual Link Analysis	Enable manual construction of link charts to provide a human-led audit trail and avoid "black box" controversy (IBM i2 Insight).

National Models of Excellence

- **France (CNIL AI Guidance):** Use CNIL's templates for reconciling AI with GDPR, specifically their frameworks for transparency and facilitating data subject rights.
- **Germany (Security-by-Design):** Adopt the German model of integrating cybersecurity into national industrial policy, emphasizing security-by-design for critical national infrastructure (CNI).

- **The Netherlands (RAN & Supervision):** Follow the Dutch "Report AI & Algorithms Netherlands" (RAN) model for proactive supervision of algorithmic risks and societal discrimination monitoring.

6. Final Recommendations for Architectural Compliance

1. **Harmonize Cross-Regime Risk Assessments:** Align risk assessment criteria between the DSA (content hosting) and AI Act (content generation) to prevent "dispersed enforcement" and regulatory gaps.
2. **Operationalize "Whole-of-Society" Resilience:** Design architecture that supports media literacy. The system must provide tools to recognize social engineering and "pig-butchering" scams, reducing susceptibility to psychological manipulation.
3. **Embed Regulatory Sandboxes for SMEs:** Actively utilize sandboxes to mitigate the significant annual costs of harmonized standards and facilitate technical compliance for smaller consortium partners.
4. **Integrate Reputation Management into Drills:** Technical incident response plans must include public communication and media response drills (modeled on **Cyber Shield OpEx**) to preserve trust during information operations.
5. **Mandate Tamper-Evident Accountability:** Every instance of data access or modification, especially in LED mode, must be recorded via **hash-chained write-once logs** to ensure absolute traceability for judicial and administrative review.

References

1. Interplay between the AI Act and the EU digital legislative framework. Parliamentary Study. Policy Department for Transformation, Innovation and Health Directorate-General for Economy, Transformation and Industry. European Parliament, October 2025. https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf
2. Multilayer Framework for Good Cybersecurity Practices for AI. ENISA Recommendation. June 2023. https://www.enisa.europa.eu/sites/default/files/publications/Multilayer%20Framework%20for%20Good%20Cybersecurity%20Practices%20for%20AI.pdf
3. Progress Report on the Digital Rulebook Implementation. Commission Policy. European Commission. September 2025. https://commission.europa.eu/document/download/68237940-a9e3-460c-bf49-932d432a6bba_en?filename=VIRKKUNEN_APR_SPI_2025_70_EN.pdf
4. 4. "Commission opens consultation on revising EU Cybersecurity Act", press release. European Commission. April 2025. https://digital-strategy.ec.europa.eu/en/news/commission-opens-consultation-revising-eu-cybersecurity-act
5. Kilian R, Jäck L, Ebel D. European AI Standards – Technical Standardisation and Implementation Challenges under the EU AI Act. European Journal of Risk Regulation. 2025;16(3):1038-1062. doi:10.1017/err.2025.10032
6. 8. Union Rolling Work Programme for European cybersecurity certification. Policy and Legislation. February 2024. https://digital-strategy.ec.europa.eu/en/library/union-rolling-work-programme-european-cybersecurity-certification
7. 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
8. Council Conclusions on the Future of Cybersecurity. Council of the EU. May 2024. https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf
9. ENISA NIS360 2024 report: A comprehensive look at cybersecurity maturity and criticality of NIS2 sectors. March 2025. https://www.enisa.europa.eu/news/enisa-nis360-2024-report
10. ENISA Threat Landscape (ETL). October 2025. https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf
11. 2024 Report on the State of Cybersecurity in the Union. December 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf
12. "European Democracy Shield and EU Strategy for Civil Society pave the way for stronger and more resilient democracies". Press Release. European Commission. November 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660
13. European Parliament Motion for a Resolution on Hybrid Provocations. European Parliament. October 2025. https://www.europarl.europa.eu/doceo/document/B-10-2025-0437_EN.pdf
14. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats. Joint staff working document. European Commission. October 2024. https://defence-industry-space.ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF
15. 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

16. Guidance on Generative AI, strengthening data protection in a rapidly changing digital era. European Data Protection Supervisor. October 2025. https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-10-28-guidance-generative-ai-strengthening-data-protection-rapidly-changing-digital-era_en
17. First EDPS Orientations for EUIs using Generative AI. European Data Protection Supervisor. June 2024. https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en
18. Guidelines on the scope of obligations for providers of General-Purpose AI (GPAI) models. July 2025. https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act
19. Guidelines on the AI system definition. February 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application
20. 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
21. General-Purpose AI Code of Practice. July 2025. https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
22. C-634/21 (SCHUFA). Automated Decision-Making & AI Ethics (GDPR Art. 22). December 2023. https://curia.europa.eu/juris/document/document.jsf;jsessionid=0EE9D6699C75E48B9657DC80D9166286?text=&docid=282187&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8119755
23. 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
24. 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
25. C-446/21 (Meta Platforms Ireland). Data Minimization and Profiling (GDPR). October 2024. https://curia.europa.eu/juris/document/document.jsf?text=&docid=290674&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8907758
26. C-203/22 (Dun & Bradstreet Austria GmbH). GDPR Article 15 (Right of Access) & Trade Secrets in Automated Decision-Making. February 2025. https://curia.europa.eu/juris/document/document.jsf?text=&docid=297932&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8125471
27. C-200/23 (Agentsia po vpisvaniyata v OL). Non-Material Damage and Loss of Control (GDPR Art. 82). 2024. https://curia.europa.eu/juris/document/document.jsf?text=&docid=290701&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1164237
28. National Cybersecurity Status Report 2024 (Nacionalinė kibernetinio saugumo būklės ataskaita 2024). https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2024.pdf
29. Report on the national cybersecurity exercise "Cyber Shield OpEx 2024" (Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas OpEx 2024" ataskaita). https://www.nksc.lt/doc/KS2024_OPEX_Pratybu_ataskaita.pdf
30. Resolution of the Seimas of the Republic of Lithuania "On the Principles of the Use of Artificial Intelligence Technologies in the Public Sector" (Lietuvos Respublikos Seimo rezoliucija „Dėl dirbtinio intelekto technologijų naudojimo viešajame sektoriuje principų"). TAR, 2024-05-16, Nr. 8947. https://www.e-tar.lt/portal/lt/legalAct/611a93c0135e11efbcbfb318996800a8
31. Methodological information (guidelines, recommendations, etc.) of the State Data Protection Inspectorate (Valstybinės duomenų apsaugos inspekcijos metodinė informacija – gairės, rekomendacijos ir kt.). https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/work/

32. 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
33. 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
34. 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 and https://www.bmftr.bund.de/DE/Forschung/Schluesseltechnologien/KuenstlicheIntelligenz/KiAktionsplan/kiaktionsplan_node.html
35. 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
36. 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
37. Guidelines on AI Literacy. https://www.autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-ai-geletterdheid
38. Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
39. AI Act Service Desk. Fundamental Rights Impact Assessment: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-27
40. General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
41. NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
42. The Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847
43. Digital Services Act: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

Finansuoja Europos Sąjunga
NextGenerationEU
Mykolo Romerio universitetas
NAUJOS KARTOS LIETUVA

Editor
<<Main Editor>>

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

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

Disclaimer