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: Deployment Requirements***

Modeling According to the Principles of Privacy by Design and Privacy by Default: Deployment 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.

While the pre-deployment phases focus on engineering privacy and security into the system's architecture, the deployment and operational phase is where these technical safeguards are activated, governed, and legally operationalized by the end-user entity. Deployment according to "Privacy by Design" and "Privacy by Default" principles demands that the system's runtime environment, user workflows, and maintenance protocols continuously uphold data protection and cyber resilience.

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

1. Regulatory Foundation and Deployment Scope

The Hybrid Information Psychological Societal Threats Handling System (HIPSTer) operates under a dual regulatory regime. Deployment compliance is determined by the legal status of the operating entity and the specific purpose of the data processing. Activities conducted by private sector entities, research institutions, and public administrations for general threat monitoring are governed by the **General Data Protection Regulation (GDPR)**. Conversely, processing performed by "competent authorities" (e.g., the Lithuanian Police or State Security Department) for the prevention, investigation, or prosecution of criminal offenses falls under the **Law Enforcement Directive (LED)**, as transposed into national law.

Legal Basis for OSINT and SocMINT Data Collection

Regulatory Regime	Legal Basis (Primary)	Deployment Application for OSINT/SocMINT
GDPR (Private/Research)	Article 6(1)(f): Legitimate Interests	Requires a structured Legitimate Interest Assessment (LIA). Processing must be necessary for hybrid threat detection and balanced against subject rights.
GDPR (Public Sector)	Article 6(1)(e): Public Task	Applicable to authorities with a statutory mandate for national cybersecurity, provided the task is defined in Union or Member State law.
LED (Competent Authorities)	Articles 4-10 LED	Must be strictly necessary for a specific criminal justice purpose. Requires a clear technical distinction between factual data and intelligence analyses (Art. 7 LED).

2. Core Requirements for Privacy by Design (PbD) in Deployment

To satisfy Article 25 of the GDPR, HIPSTer integrates technical and organizational measures (TOMs) into its core architecture. As a Privacy Architect, I mandate that these measures move beyond policy to hard-coded technical enforcement.

- **Data Minimization & Provenance:**
  - **Ingestion Filters:** Deployment utilizes Python-based crawlers with granular metadata filters to ingest only publicly available information (PAI).
  - **Pipeline Processing:** The architecture employs **Kafka** for message queuing, ensuring data streams are segregated at the point of entry. **Pandas and Spark** are utilized for automated cleaning and the removal of irrelevant personal identifiers before storage.
  - **Schema Control:** Data is stored in **Elasticsearch/OpenSearch** using strict, schema-controlled environments that prevent the accidental ingestion of non-target data fields.
- **Encryption Standards:**
  - **Data at Rest:** All databases and backups are encrypted using AES-256. Key management must be handled via an **EU-region Hardware Security Module (HSM)** or a dedicated Key Management Service (KMS).
  - **Data in Transit:** Enforcement of TLS 1.3 for all internal module communication and external API calls.
- **Access Control & Siloing:**
  - **RBAC & MFA:** Standard Role-Based Access Control is bolstered by mandatory Multi-Factor Authentication (MFA).
  - **ABAC for LED-mode:** For law enforcement deployments, **Attribute-Based Access Control (ABAC)** is implemented to ensure that access to intelligence analyses is restricted based on specific investigation clearance levels.

3. Privacy by Default: Operational Configuration

"Privacy by Default" ensures that the highest level of data protection is the system's baseline state. The following **Default Configuration Rules** are mandatory for any HIPSTer instance:

1. **Hard-Coded Legal Stream Segregation:** By default, the system architecture maintains separate data silos for GDPR-governed and LED-governed data. This is enforced at the database level through schema isolation to prevent unlawful data mixing.
2. **Automated Retention Enforcement:** The system defaults to purpose-specific storage periods. Data is automatically flagged for erasure or anonymization upon reaching the end of its analytical lifecycle, driven by automated scripts.
3. **Pseudonymization of Special-Category Data:** OSINT feeds revealing sensitive attributes (political opinions, religious beliefs) are automatically pseudonymized at the ingestion layer unless a high-level override is granted for a specific, documented investigation.
4. **Log Integrity via Hash Chaining:** All data consultations, modifications, and disclosures are recorded in tamper-evident, write-once logs. To ensure auditability, the system uses **hash chaining** to link log entries, making unauthorized deletions or alterations detectable.

4. High-Risk AI Compliance (EU AI Act Integration)

HIPSTer is classified as a **high-risk AI system** under Annex III of the EU AI Act, specifically within the categories of law enforcement and public security.

High-Risk AI Deployment Mandates

Requirement Area	AI Act Article	Deployment Action Item
Risk Management	Article 9	Maintain a continuous, iterative risk register covering the full lifecycle, including red-teaming for "jailbreak" attempts.
Data Governance	Article 10	Conduct automated bias scans on training/validation sets to ensure representativeness and mitigate discriminatory outcomes.
Technical Documentation	Article 11	Maintain auto-generated model cards and data lineage records; documentation must be ready for regulatory inspection.
Transparency	Article 13	Deploy role-specific explainability dashboards providing clear rationales for automated threat scores.
Human Oversight	Article 14	Implement "human-in-the-loop" protocols; high-impact actions (e.g., law enforcement escalation) require manual validation.
Accuracy & Security	Article 15	Conduct regular adversarial testing to defend against model inversion and data poisoning.
Rights Assessment	Article 27	Mandatory **Fundamental Rights Impact Assessment (FRIA)** for all public sector deployments prior to operational use.

5. The Ethical, Legal, and Social Aspects (ELSA) Deployment Framework

Transparency is not a "one-size-fits-all" requirement. The HIPSTer ELSA framework utilizes a tiered disclosure model to satisfy both operational needs and legal mandates like the right to explanation.

User-Centric Transparency Matrix

User Role	Disclosure Requirements
Operational Users	Confidence scores, key indicators/signals contributing to a flag, indicator reliability metrics, and uncertainty estimates.
Data Subjects	Meaningful information about the logic involved in automated processing and the weighting of data used to categorize them (per CJEU C-203/22).
Regulators/Auditors	Detailed training data provenance, bias audit logs, performance metrics, and technical documentation of the model's architecture.

6. National Implementation: The Lithuanian Context

In Lithuania, HIPSTer must align with the Law on Legal Protection of Personal Data (ADTAI) 2024 amendments and the Law on Cyber Security, which transposes the NIS2 Directive.

Lithuanian "Gold-Plating" and Compliance Obligations

- **NCSC Mandatory Reporting:** Incidents must be reported to the National Cyber Security Centre on a strict schedule: **24h** (early warning), **72h** (detailed report), and **1 month** (final remediation report).
- **Managerial Liability:** The 2024 Law on Cyber Security introduces **personal responsibility for managers** in cases of gross negligence regarding cybersecurity measures.

- **Investigative Obligations:** Per *Beizaras and Levickas v. Lithuania*, authorities are legally bound to investigate credible reports of hate speech; HIPSTer detections provided to LEAs must be documented and traceable to support this.
- **Contextual Intent:** Per Supreme Court case *2K-86-648/2016*, AI models must distinguish between shocking content and actual intent to incite hatred; human review is mandatory for borderline cases.

7. Operational Challenges and Case Study Insights

Insights from platforms like Palantir and Recorded Future highlight critical risks that HIPSTer deployments must mitigate:

- **The "Trade Secret" Trap vs. Right of Access:** Per CJEU C-203/22 (*Dun & Bradstreet*), practitioners cannot use trade secrets as a blanket shield. They must provide the principles and logic of data weighting to data subjects while protecting the specific code.
- **The Autonomous Operations Conflict:** As seen in Recorded Future's roadmap, transitioning toward **"Autonomous" operations** creates a significant conflict with **Article 22 of the GDPR**. Machine-speed responses without human intervention risk being legally invalid for high-impact decisions.
- **The "Black Box" Auditability Gap:** Palantir case studies reveal that government users can sometimes disable audit features. HIPSTer must enforce **non-bypassable, write-once logging** to ensure legal accountability.
- **Adversarial Red-Teaming:** Deployment must account for model poisoning, where adversaries intentionally feed corrupt data into OSINT streams to degrade the system's detection accuracy.

8. Deployment Compliance Checklists

Pre-Deployment Readiness

- [ ] Completion of a Data Protection Impact Assessment (DPIA) under Art. 35 GDPR.
- [ ] Completion of a Fundamental Rights Impact Assessment (FRIA) for public sector entities.
- [ ] Execution of a Legitimate Interest Assessment (LIA) for private sector use.
- [ ] Formal designation of a Data Protection Officer (DPO).

Technical Integrity

- [ ] Verification of AES-256 encryption at rest (KMS/HSM) and TLS 1.3 in transit.
- [ ] Implementation of **Log Integrity** via hash-chaining and tamper-evident storage.
- [ ] Validation of **API Security** and mandatory Multi-Factor Authentication (MFA).
- [ ] Confirmation of hard-coded data stream segregation (GDPR vs. LED modes).

Human Oversight

- [ ] Establishment of "human-in-the-loop" escalation workflows for high-risk decisions.
- [ ] Configuration of the Explainability Dashboard for operational users.
- [ ] Setup of 24/7 incident monitoring and automated NCSC reporting channels.
- [ ] Documentation of human-led audit procedures for AI-generated scores.

9. Concluding Strategic Insights

HIPSTer deployment marks a shift toward a **socio-technical paradigm**. Compliance is no longer just about IT safety; it is a tool for **Reputation Management** and the preservation of **Democratic Trust**. A technical failure—be it a biased flag or a data leak—now directly impacts social cohesion and the rule of law.

Strategic Compliance Pillars for HIPSTer

1. **Iterative Lifecycle Governance:** Risk management and bias monitoring must be continuous, not static, to adapt to evolving adversarial tactics and narrative shifts.
2. **Explainability as a Legal Safeguard:** Radical transparency regarding algorithmic logic is the only defense against the "Trade Secret" trap and the "Right to Explanation" under CJEU jurisprudence.
3. **Whole-of-Society Resilience:** Practitioners must integrate public communication and media response teams into cyber exercises (mirroring Lithuania's "Cyber Shield OpEx"). Defense is incomplete without a plan to maintain public trust during a disinformation crisis.

Annex: HIPSTer System Operational Deployment and Compliance Framework

This framework provides the strategic operational requirements for the deployment of the Hybrid Information Psychological Societal Threats Handling System (HIPSTer). As a platform utilizing advanced OSINT, SocMINT, and AI to counter Foreign Information Manipulation and Interference (FIMI), its implementation must bridge the gap between technical scalability and the stringent requirements of the EU AI Act, GDPR, NIS2, and the Law Enforcement Directive (LED).

1. HIPSTer Deployment Lifecycle: Key Operational Stages

The implementation follows a modular, risk-aware lifecycle designed to ensure technical robustness and regulatory alignment.

Stage 1: Socio-Technical Design & Risk Assessment

- **Description:** This stage treats threats as complex socio-technical harms rather than simple IT failures. It identifies attacker motives and assesses the risk of eroding democratic trust or violating fundamental rights.
- **Practical Deployment Steps:**
  - **Adversary Profiling:** Create detailed psychological profiles of state-aligned actors and "cyberwarriors" to understand motives and objectives.
  - **Prohibited Vulnerability Screening:** Map system inputs against AI Act Article 5 to ensure the system does not exploit vulnerabilities related to age, disability, or socio-economic circumstances.
  - **Fundamental Rights Impact Assessment (FRIA):** Conduct a mandatory FRIA (Art. 27) evaluating the impact on freedom of expression (ECHR Art. 10) and non-discrimination.

Stage 2: Data Preparation and Bias Mitigation

- **Description:** This stage focuses on the normalization of OSINT data while resolving the "Bias Paradox"—the technical need for sensitive data to correct algorithmic discrimination versus GDPR prohibitions.
- **Practical Deployment Steps:**
  - **Operational Mode Segregation:** Implement differentiated UI/UX modes ("GDPR Mode" for research vs. "LED Mode" for criminal investigations) to prevent unlawful data mixing.
  - **Article 10 Safeguard Implementation:** Process special categories of data (e.g., political opinions) strictly for bias monitoring with technical locks preventing transmission to third parties.
  - **Source Provenance Tagging:** Utilize Kafka message headers to tag data with its legal basis and "manifestly made public" status (Art. 9(2)(e) GDPR).

Stage 3: Adversarial Testing & "Red-Teaming"

- **Description:** Defensive measures are tested against sophisticated manipulation, including "jailbreak" attempts on LLMs and attempts to corrupt the system's intelligence graph.

- **Practical Deployment Steps:**
  - **Adversarial Model Defense:** Conduct red-teaming focused specifically on "model inversion attacks" and "model poisoning" where adversaries attempt to corrupt training sets.
  - **Synthetic Media Detection:** Test the accuracy of NLP and transformer-based models in identifying AI-generated deepfakes and automated social engineering campaigns.
  - **National Drill Integration:** Participate in exercises like "Cyber Shield OpEx" to test technical recovery alongside reputation management.

Stage 4: Operational Monitoring and Rapid Response

- **Description:** Real-time monitoring ensures the system remains accurate post-deployment, preventing "model drift" and ensuring human accountability.
- **Practical Deployment Steps:**
  - **Human-in-the-Loop (HITL) Protocols:** Establish mandatory human review for high-impact escalations to ensure no autonomous "predictive policing" occurs.
  - **Narrative Shift Detection:** Use graph analytics (TigerGraph) to detect shifts in FIMI narratives in real-time.
  - **Drift Telemetry:** Monitor for "automation bias" and performance degradation to prevent the reinforcement of belief bubbles or discriminatory outcomes.

2. Comprehensive Compliance & Readiness Checklists

Table 1: Data Protection & GDPR Compliance

Requirement	Legal Basis / Case Law	Operational Action Item
Data Minimization	Art. 5(1)(c); C-446/21	Configure Spark-based processing to filter PII not strictly necessary for threat detection.
Right of Access & Explanation	Art. 15; C-203/22	Implement **Explainability Dashboards** to reveal data weighting logic without exposing proprietary weights.
Liability for Loss of Control	Art. 82; C-200/23	Implement tamper-evident logging and real-time alerts to mitigate even temporary "loss of control" over data.
Automated Decision Oversight	Art. 22; C-634/21	Ensure probability scores (e.g., risk levels) require meaningful human review before consequential use.
Purpose Limitation	Art. 5(1)(b); LED Art. 4	Maintain strict separation between research/OSINT data and investigative/LED data streams.

Table 2: AI Act High-Risk System Mandates

Requirement (Arts. 9-15, 27)	System Function Affected	Verification Method
Risk Management (Art. 9)	Full Lifecycle	Documented risk register including "socio-technical" harms (e.g., trust erosion).
Data Governance (Art. 10)	Training & Validation Layer	Bias scans and documentation of dataset representativeness; Art. 10 safeguard audits.
Technical Documentation (Art. 11)	System Architecture	Auto-generated "Model Cards" and architecture diagrams (Kafka/Spark/Elasticsearch).

Transparency (Art. 13)	User Interface (UI/UX)	Dashboards explaining logic, limitations, and confidence scores to operators.
Human Oversight (Art. 14)	Response Layer	Mandatory "Override" and "Stop" protocols for AI-generated recommendations.
Accuracy & Security (Art. 15)	AI/Analytics Layer	Red-teaming reports for model poisoning and jailbreak resilience.

Table 3: Cybersecurity & Resilience (NIS2/CRA/DSA)

Security Measure	Target Threat	Implementation Status (Reporting Tier)
Tiered Incident Reporting	Data Breaches / Sabotage	**24h:** Early Warning; **72h:** Detailed Report; **1 Month:** Final Report.
FIMI Detection Integration	Foreign Interference	Integration with SIEM for real-time alerting on coordinated influence campaigns.
Supply-Chain Security	Model Poisoning	Secure SDLC; audit of AI model provenance and vendor assessment.
Trusted Flagger Format	Disinformation	DSA-compliant substantiated reports for platform notification-and-action.
Robustness Testing	Adversarial AI	Implementation of AES-256 and secure containerization (Docker/Kubernetes).

3. Critical Operational Challenges in Hybrid Threat Deployment

Challenge 1: The Regulatory Complexity/Bias Paradox Trigger: Interaction between AI Act Art. 10 and GDPR Art. 9. The AI Act mandates the use of sensitive personal data to monitor and correct bias, yet the GDPR generally prohibits such processing. Deployment teams face "dispersed enforcement" risks where failing to monitor bias leads to discriminatory targeting, while monitoring might trigger GDPR non-compliance.

Challenge 2: The "Subliminal" vs. "Persuasion" Gap Trigger: AI Act Art. 5 (Prohibited Practices). HIPSTer utilizes counter-narratives to mitigate FIMI. However, legal specificity is lacking regarding the threshold where "lawful persuasion" becomes "prohibited manipulation" or "subliminal distortion." Automated campaigns must not impair informed decision-making or exploit socio-economic vulnerabilities.

Challenge 3: Transparency vs. Security (The Trade Secret Trap) Trigger: CJEU Case C-203/22 (Dun & Bradstreet). Data subjects have a right to the "logic involved" in profiling. While developers cite trade secrets, the CJEU ruled these cannot be used as a blanket shield. Practitioners must deploy **Explainability Dashboards** that provide enough detail (e.g., which data categories were weighted) to satisfy the court without enabling adversaries to "poison" the model.

Challenge 4: The Technical Standardization Lag Trigger: AI Act Implementation Period. There is an "insufficient implementation period" (currently < 6 months) for the ~30 harmonized standards required for compliance. This creates a high risk of inconsistent enforcement across Member States, as technical criteria for "robustness" or "accuracy" remain subjective until standardized.

4. Strategic Recommendations for Overcoming Deployment Barriers

1. **Harmonize Enforcement Mechanisms:** Practitioners must align risk assessments between the **Digital Services Act (DSA)** for content hosting and the **AI Act** for content generation to ensure consistent treatment of FIMI threats across the value chain.
2. **Operationalize Reputation Management:** Beyond technical recovery, agencies should use exercises like "Cyber Shield OpEx" to test the ability to maintain public trust during **content distortion** events. Success is measured by the efficacy of public communication, not just system uptime.
3. **Implement Lifecycle Risk Management:** Move beyond one-off conformity assessments. Implement continuous monitoring to detect "automated social engineering" and "model drift," adapting the system to the evolving tactics of state-aligned threat actors.
4. **Utilize Regulatory Sandboxes:** Leverage specialized environments for SMEs and research partners to test technical compliance with emerging standards, providing a "safe harbor" to refine models before full-scale deployment.

5. Technical Architecture & Security Controls Reference

Layer	Primary Function	Security Control	Regulatory Alignment
Collection	OSINT/SocMINT Ingestion	TLS 1.3, Python-based crawlers, Kafka Queues	GDPR (Art. 25), LED
Processing	Cleaning & Normalization	Spark, Elasticsearch, AES-256, RBAC	GDPR, NIS2, LED
AI/Analytics	FIMI & Bias Detection	TigerGraph, SHAP/LIME (XAI), PyTorch	AI Act (High-Risk)
Interface	Dashboards & Alerts	Multi-factor Auth (MFA), Explainability Dashboards	Art. 15 GDPR, Art. 13 AI Act

6. Deployment Glossary and Reference Links

Essential Abbreviations

- **AI:** Artificial Intelligence
- **DSA:** Digital Services Act
- **FIMI:** Foreign Information Manipulation and Interference
- **GDPR:** General Data Protection Regulation
- **LED:** Law Enforcement Directive (Directive (EU) 2016/680)
- **OSINT / SocMINT:** Open Source / Social Media Intelligence
- **NKSC / NCSC:** National Cyber Security Centre

Primary Legal Authorities

- **EU AI Act (Regulation (EU) 2024/1689)**
- **NIS2 Directive (Directive (EU) 2022/2555)**
- **Lithuanian Law on Cyber Security (2024 Amendments)**
- **National Security Strategy of Lithuania (2017)**

- **CJEU Case Law:** C-203/22 (Trade Secrets/Access), C-634/21 (Automated Scoring), C-200/23 (Non-Material Damage/Loss of Control).
- **ENISA Threat Landscape (ETL) 2025**

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