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: System Analysis Requirements***

Finansuoja Europos Sąjunga NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Modeling According to the Principles of Privacy by Design and Privacy by Default: System Analysis 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 comprehensively fulfill the requirements of Privacy by Design, Security by Design, and the broader regulatory landscape (including the GDPR, EU AI Act, NIS2, and NATO standards), system analysis and modeling must embed legal and technical safeguards into the system's core architecture before deployment.

Below is an in-depth elaboration of the key stages and specific technical requirements that must be accounted for during system analysis.

1. Regulatory Jurisdictional Analysis and Scope

The HIPSTer platform operates within a tiered regulatory environment where jurisdictional boundaries are determined by the entity's mandate and the specific purpose of data processing. Compliance requires strict adherence to the criteria of transition between the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), and National Security exemptions.

Jurisdictional Regimes under Art. 2(2)(a) GDPR and Art. 1(1) LED

Legal Regime	Primary Governing Law	Applicable HIPSTer Partners/Activities	Transition Criteria
GDPR-Governed	Regulation (EU) 2016/679	Consortium partners (Universities, KTU, MRU), private entities (ELSIS PRO), and public bodies acting for research or general security.	Default regime for all processing unless a specific "Competent Authority" mandate for criminal justice applies.
LED-Governed	Directive (EU) 2016/680 (Transposed into Lithuanian Law)	Competent authorities (Police, FNTT, Customs) when processing for the prevention, investigation, or prosecution of criminal offenses.	Triggered only when a Competent Authority processes data for specific criminal justice purposes under Article 1(1) LED.
National Security-Exempt	Lithuanian Law on Intelligence; National Security Strategy (2017)	State Security Department (VSD) and Military Intelligence (AOTD) acting under Article 4(2) TEU.	Strictly limited to activities performed for the **exclusive** purpose of national security.

The Dual-Use Complexity and National Security Exemption

Under Article 4(2) of the Treaty on European Union, national security remains the sole responsibility of the Member State. However, the HIPSTer platform must navigate the "Dual-Use" trap: if the system is used for both civilian cybersecurity (GDPR/AI Act regulated) and national security (Exempt), it **cannot** claim a blanket exemption. The system **must** implement technically enforced operational modes. Any processing not strictly and exclusively for national security must comply with the EU AI Act's high-risk requirements. Integration with the Lithuanian Law on Intelligence requires that any data revealed to intelligence bodies from civilian streams must follow secure, legally-authorized "hand-over" protocols rather than direct, unregulated access.

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

In accordance with Article 25 GDPR, the HIPSTer lifecycle must integrate "Privacy by Design" as a technical specification, not merely a policy statement.

2.1. Core PbD Technical Requirements

1. **Data Minimization for OSINT/SocMINT:** The system **must** implement ingestion filters that strip PII from Open-Source Intelligence (OSINT) at the point of collection. Only "Analytical Indicators" (patterns) and "Identifiers" strictly necessary for threat attribution may be retained.
2. **Jurisdictional Data Segregation:** The architecture **must** maintain separate data silos for GDPR-regulated research and LED-regulated law enforcement data to prevent unlawful cross-contamination and "function creep."
3. **Pseudonymization Strategy:** Systematic pseudonymization **must** be applied to all identifiers in the processing layer (Art. 4(5) GDPR). Re-identification keys must be stored in a separate, encrypted Hardware Security Module (HSM).
4. **Legal-Basis Tagging:** Every ingested data point **must** be tagged with its specific legal basis (e.g., Art. 6(1)(f) Legitimate Interest for private sector or Art. 6(1)(e) Public Task for public authorities).

2.2. Privacy by Default

As mandated by the 2024 amendments to the Lithuanian Law on Legal Protection of Personal Data (ADTAI), the platform **must** implement:

- **Mandatory Processor Oversight:** Public sector contractors **must** adhere to stricter auditing obligations than private-sector counterparts.
- **DPIA-Defined Retention:** The system **must** hard-code retention limits. Once data exceeds the storage period defined in the DPIA, automated "deletion-by-default" triggers must execute.
- **Pre-Complaint Procedure Alignment:** For public-sector deployments involving video or OSINT-based monitoring, the interface **must** support the mandatory pre-complaint procedures overseen by the State Data Protection Inspectorate (SDPI).

3. Ethical and Social Requirements (ELSA) Framework

HIPSTer adopts a **"Socio-Technical" paradigm** (ENISA 2023), recognizing that technical failures in AI threat detection result in direct harms to democratic trust and fundamental rights.

3.1. AI Ethics and Human-in-the-Loop (HITL)

- **Human-Led Audit Trail:** All high-impact decisions (e.g., flagging an account for law enforcement) **must** be accompanied by a manual review. The system must record the identity of the human reviewer and their rationale to prevent "autonomous predictive policing."
- **Psychological Profiles of Attackers:** Design stages **must** incorporate behavioral modeling of potential adversaries to understand motives and mitigate "socio-technical" vulnerabilities such as trust manipulation.
- **Operational Explainability:** Models **must** provide confidence scores and SHAP/LIME-based rationales for threat scores, tailored to the operator's level of expertise.

3.2. Safeguarding ECHR Article 10 (Freedom of Expression)

To prevent the "chilling effect" on public discourse, the system **must** implement:

- **Context-Sensitive NLP:** Models **must** be specifically trained on datasets that distinguish between harmful incitement and legitimate expression, including **satire, political debate, and journalistic reporting**.
- **Media Sensitivity Thresholds:** Automated sensitivity "damping" for verified media outlets and public-interest accounts is **mandatory** to prevent accidental suppression of legitimate news.

4. Systematic Analysis of Data Protection Impact (DPIA)

Under Article 35 GDPR, HIPSTer triggers a high-risk classification due to large-scale monitoring and profiling.

4.1. High-Risk Criteria and Safeguards

- **Systematic Profiling:** The platform evaluates behavioral patterns (Art. 4(4) GDPR), requiring rigorous accuracy checks.
- **Special Category Data:** Incidental collection of political/religious views requires strict filtering under Art. 9 GDPR.
- **Technical Safeguards:** The system **must** include defenses against **Model Inversion Attacks** and **Data/Model Poisoning** (adversarial attempts to corrupt training data).

4.2. DPO and SDPI Consultation

The Data Protection Officer (DPO) **must** have "read-only" access to compliance logs. If the DPIA identifies high residual risks that cannot be mitigated by technical controls, the consortium **must** engage in **Article 36 consultation** with the Lithuanian SDPI prior to processing.

5. AI Act Compliance for High-Risk Systems

HIPSTer is classified as a "High-Risk AI System" under Annex III of the EU AI Act (Regulation 2024/1689). **Full compliance is mandatory by August 2, 2027.**

- **Risk Management (Art. 9):** A continuous, documented risk-management cycle **must** be established, involving iterative red-teaming against "jailbreak" attempts.
- **Data Governance (Art. 10):** Training and validation datasets **must** be audited for statistical representativeness to eliminate bias against protected groups.
- **Technical Documentation (Art. 11):** The system **must** auto-generate "Model Cards" and maintain immutable data lineage records.
- **Fundamental Rights Impact Assessment (Art. 27):** Public-sector deployments **must** conduct a FRIA. This assessment **must** explicitly measure the "chilling effects on public discourse" and potential for discriminatory targeting.
- **GPAI Code of Practice:** While HIPSTer is a downstream system, it **must** align with the GPAI Code of Practice for any integrated foundation models.

6. Technical Architecture and Security Specifications

6.1. Layered PbD Architecture

Layer	Function	Technical PbD Feature Required
1. Data Collection	Multi-source ingestion	**Legal-Basis Tagging:** Metadata tags for source and jurisdiction (GDPR vs LED).
2. Data Processing	Normalization & storage	**Automated Retention Enforcement:** Hard-coded deletion rules via API.
3. AI/Analytics	Detection & attribution	**Explainable AI (XAI) Engine:** Mandatory scoring rationales for every alert.
4. Decision/Response	Alerting workflows	**Human-in-the-Loop Escalation:** Mandatory manual override for high-impact alerts.
5. Interface	Dashboards & exports	**Jurisdictional RBAC:** UI views restricted by user role and legal mandate.

6.2. Security Specifications

- **Encryption: AES-256** at rest; **TLS 1.3** in transit with EU-only key management.
- **Tamper-Evident Logging:** LED-compliant, "write-once" logs **must** implement **Hash Chaining** and **Timestamping** to ensure the integrity of the audit trail for a minimum of 3 years.
- **Resilience:** Integration with SIEM for real-time detection of model poisoning or adversarial manipulation.

7. Judicial Precedents and Evolving Liability

- **C-634/21 (SCHUFA):** Limits automated scoring. HIPSTer **must not** produce scores that lead to automated legal effects without human intervention.
- **C-203/22 (Dun & Bradstreet):** The "Trade Secret Trap." Intellectual property **cannot** be used to withhold the logic of threat scores from data subjects. The system **must** be capable of explaining its "weighting" logic.
- **C-200/23 (Agentsia):** Even a **short-term "loss of control"** constitutes non-material damage. This places a technical burden on Layer 2 to ensure zero-latency enforcement of deletion rules.

8. Implementation Challenges and Strategic Recommendations

8.1. Practical Challenges

1. **Regulatory Complexity:** Balancing AI Act Art. 10 (bias monitoring) with GDPR Art. 9 (sensitive data prohibition).
2. **Subliminal vs. Persuasion:** Distinguishing "lawful counter-persuasion" from "prohibited behavioral manipulation" (AI Act Art. 5).
3. **Transparency vs. Security:** Providing enough logic to satisfy Art. 15 GDPR without enabling adversaries to bypass detection (the "poisoning" risk).

8.2. Strategic Recommendations

- **Regulatory Sandboxes:** Engage with the Lithuanian SDPI sandbox to validate high-risk AI features before the 2027 deadline.
- **"Whole-of-Society" Resilience:** Shift from purely technical defense to a societal approach by integrating media literacy indicators into threat models.
- **Harmonize Enforcement:** Align risk metrics between the AI Act (generation) and the DSA (hosting) to ensure consistent threat treatment.

9. Master Compliance Checklist

Regulatory Area	Requirement/Provision	HIPSTer Technical/Operational Implementation
GDPR	PbD (Art. 25)	Analytical indicator pseudonymization; Jurisdictional silos.
GDPR	Right of Access (Art. 15)	Explainability dashboards; No "Trade Secret" blanket shield.
LED	Traceability (Art. 25)	Write-once logs using **Hash Chaining** and **Timestamping**.
AI Act	Risk Management (Art. 9)	Continuous risk register; Red-teaming against model inversion.

AI Act	Data Governance (Art. 10)	Statistical bias audits; Representative training sets.
NIS2	Incident Reporting (Art. 23)	**24h Early Warning / 72h Notification** SIEM workflows.
DSA	Notice-and-Action (Art. 14)	Precise, substantiated "Trusted Flagger" notification formats.
ADTAI 2024	Public Sector Accountability	DPO-led oversight of high-risk public-sector analytics.
Data Act	International Access	Technical safeguards against unlawful third-country data requests.
CRA	Adversarial Resilience	Hardened secure-development lifecycle against data poisoning.

Annex: HIPSTer System Analysis – Stages, Compliance, and Operational Challenges

This annex provides the formal Requirement-to-Measure Mapping and operationalized controls for the Hybrid Information Psychological Societal Threats Handling System (HIPSTer). It serves as the authoritative blueprint for ensuring regulatory interoperability across EU and Lithuanian jurisdictions.

1. HIPSTer System Analysis Lifecycle Stages

The implementation of the HIPSTer system is governed by four distinct lifecycle stages, designed to transition from high-level socio-technical risk mapping to real-time operational resilience.

1. **Socio-Technical Design & Risk Assessment**
    - **Description:** This stage moves beyond legacy IT failure models to evaluate threats as social and psychological harms affecting democratic integrity.
    - **Practical Steps:** Architects must develop "psychological profiles" of anticipated adversaries, specifically analyzing the motives and objectives of state-sponsored attackers and cyberwarriors. Risk assessments must evaluate the "chilling effects" on free expression and democratic trust, identifying how technical vulnerabilities translate into societal harms.
2. **Data Preparation and Bias Mitigation**
    - **Description:** Operationalizing the tension between strict data protection mandates and the technical necessity for sensitive data to ensure algorithmic fairness.
    - **Practical Steps:** Pursuant to AI Act Article 10, developers may process special categories of personal data (e.g., political opinions, ethnicity) provided such processing is a **strict necessity** and meets **proportionality** standards for bias detection and correction. All such activities must maintain strict GDPR alignment, ensuring sensitive data is isolated from general analytical workflows.
3. **Adversarial Testing**
    - **Description:** Proactive validation of system robustness against intentional manipulation, data poisoning, and model inversion.
    - **Practical Steps:** Execute adversarial "red-teaming" exercises to simulate hostile attempts at bypassing detection logic. This includes testing the model's resilience against "jailbroken" prompts and synthetic media (deepfakes) designed to deceive security analysts or corrupt the training pipeline.
4. **Operational Monitoring and Communication**
    - **Description:** Real-time oversight characterized by human-in-the-loop (HITL) control and the management of organizational reputation during active threat cycles.
    - **Practical Steps:** Deploy Security Information and Event Management (SIEM) systems integrated with automated OSINT and NLP tools for immediate detection of AI-driven social engineering. Implement **hash-chaining** for all audit logs to ensure tamper-evident evidence trails. Organizations must conduct reputation management drills (e.g., "Cyber Shield OpEx") to maintain public trust during active disinformation operations.

2. Comprehensive Compliance Checklist: Privacy by Design & Default

The following tables operationalize the requirements of the GDPR, AI Act, and the 2024 amendments to the Lithuanian Law on Legal Protection of Personal Data (ADTAI).

GDPR Privacy by Design (Art. 25) & Default

Requirement	Description	HIPSTer Measure
Privacy by Design	Architectural integration of data protection.	End-to-end encryption; purpose-specific data flows; pseudonymization of analytical indicators.
Data Minimization	Collection limited to strict necessity (Art. 5).	Metadata provenance tracking to discard irrelevant PII; automated ingestion filters for OSINT/SocMINT.
2024 ADTAI Updates	Lithuania-specific rules for public sector systems.	Enhanced transparency for public-sector digital systems; expanded mandate for SDPI in supervising high-risk analytics.
Processor Obligations	Stricter liability under 2024 ADTAI.	Implementation of standardized DPAs with specific contractor liability clauses for public authority contracts.
Default Settings	Automated application of strict privacy logic.	Default role-based access control (RBAC); automated storage limitation enforced via hard-coded retention scripts.

AI Act High-Risk System Requirements

Requirement (Art. 9-15)	Description	Implementation Action
Risk Management	Continuous, documented risk-management cycle.	Centralized risk register covering design, testing, and deployment; quarterly adversarial robustness reviews.
Data Governance	High-quality, representative, and bias-audited datasets.	Bias scans and statistical representativeness audits on training/validation data; documentation of data provenance.
Technical Documentation	Record-keeping for market surveillance authorities.	Automated generation of model cards, architecture diagrams, and version control logs for regulatory audit.
Transparency	Interpretable logic and user instructions.	Deployment of explainability dashboards (XAI) to ensure users understand the "logic" behind flagged content.
Human Oversight	Effective human-in-the-loop supervision (Art. 14).	Mandatory human review for high-impact actions; override protocols for automated recommendations.
FRIA (Art. 27)	Fundamental Rights Impact Assessment.	**Mandatory** assessment of impacts on privacy, non-discrimination, and freedom of expression before public-sector deployment.

Multi-Domain Regulatory Safeguards

Regulation	Domain	Compliance Checkpoint
LED (2016/680)	Law Enforcement	**Art. 7 Requirement:** Differentiate between factual personal data and analytical assessments/inferences in system outputs.
NIS2	Cybersecurity	24/7 incident handling; early warning (24h) and notification (72h); **Supply-chain security** for AI and cloud service providers.
DSA	Digital Services Act	"Trusted flagger" notices must be precise, substantiated, and support auditability/redress for platforms.

Cyber Resilience Act	Product Security	Protection against model poisoning and unauthorized inversion attacks; secure-by-design software development lifecycle (SDLC).

3. Practical Challenges in System Implementation

Architectural deployment of the HIPSTer system must navigate the following legal and operational conflicts:

Challenge: Regulatory Complexity (GDPR vs. AI Act) The Conflict: While AI Act Article 10 permits processing sensitive data to detect and correct bias, the GDPR generally prohibits such processing. Practitioners risk a "compliance trap" where failing to monitor bias leads to discriminatory AI, but doing so may invite GDPR enforcement.

Challenge: The "Subliminal" vs. "Persuasion" Gap The Conflict: The AI Act prohibits AI practices that use subliminal or deceptive techniques to **distort behavior** in a way that causes **significant harm**. There is currently a lack of legal specificity to distinguish lawful public-sector persuasion from prohibited manipulation in counter-disinformation campaigns.

Challenge: Transparency vs. Security (The "Trade Secret" Trap) The Conflict: Pursuant to CJEU Case **C-203/22**, the right to understand the "logic" of AI decisions is paramount. Controllers cannot use "trade secrets" as a **blanket shield** to deny access to data weighting. However, disclosing this logic may allow adversaries to reverse-engineer and "poison" the detection model.

Challenge: The Implementation and Standardization Lag The Conflict: There is an effective implementation window of less than 6 months for nearly 30 technical standards, whereas **SMEs and startups** realistically require 12 months for full alignment. This creates a risk of "dispersed enforcement" across the EEA.

4. Strategic Recommendations for Overcoming Challenges

Technical Mitigations

- **Operationalized Human Oversight:** Establish "Human-in-the-loop" as the immutable default for any decision carrying legal or significant effects.
- **Data Lineage & Lifecycle Management:** Implement **automated storage limitation** scripts and **data lineage tracking** to ensure data is deleted according to DPIA-defined retention periods.
- **Adversarial Red-Teaming:** Conduct quarterly red-team vs. blue-team exercises to identify vulnerabilities in the AI's logic before exploitation by hostile state actors.

Legal & Administrative Mitigations

- **Utilization of Regulatory Sandboxes:** Leverage national and EU sandboxes to test compliance for high-risk features against emerging standards, particularly for SMEs.
- **Standardized DPAs:** Adopt standardized Data Processing Agreements that incorporate the **2024 ADTAI amendments** to streamline public-private information sharing.
- **Fundamental Rights Impact Assessments (FRIA):** Conduct comprehensive FRIAs as a prerequisite for deployment to mitigate chilling effects on civil liberties.

Societal & Communication Mitigations

- **Stakeholder Involvement:** Involve **civil society and academia** in evaluating ethical impacts to align with the Lithuanian Seimas Resolution on AI ethics.
- **Whole-of-Society Resilience:** Support media literacy campaigns to educate the public on recognizing "pig-butchering" scams and AI-driven social engineering.
- **Reputation Management Drills:** Integrate communication teams into "Cyber Shield OpEx" style exercises to train for maintaining public trust during active hybrid crises.

5. Technical Architecture & Security Controls Reference

The following table summarizes the operationalized controls required for a "Privacy by Design" posture.

Security / Compliance Measure	Description	Technical Implementation
Encryption	Protection at rest and in transit.	AES-256 for storage; TLS 1.3 for transport; Key management via EU-region HSM/KMS with **EU-only keys**.
Access Control (RBAC)	Granular privilege management.	Cloud IAM with MFA; Attribute-Based Access Control (ABAC) to segregate LED/GDPR data streams.
Comprehensive Logging	LED/GDPR-compliant audit trails.	**Hash-chaining** and write-once logs; SIEM ingestion for real-time monitoring; 3-year retention for LED logs.
Security Audits	Continuous verification of posture.	**Quarterly internal tests**; annual third-party audits; Red-team vs. Blue-team simulation exercises.
Data Governance	Lifecycle and retention control.	**Automated retention enforcement**; DPIA-linked retention audits; data lineage tracking for all PAI/CAI ingestion.
Cross-Border Transfer	Safeguards for non-EEA exchange.	Transfer Impact Assessments (TIAs); Standard Contractual Clauses (SCCs); **MLAT verification** for LED-mode transfers.

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