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: ***AICP-FIMI***

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

Action result: ***Scientific Research Report on Personal Data Protection and GDPR Compliance***

AICP-FIMI – AI-Driven Cloud Platform to Counter Foreign Information Manipulation during Elections

Scientific Research Report on Personal Data Protection and GDPR Compliance

Field	Value
Report Identifier	AICP-MRU-WP10-FINAL-REPORT-v2.0
Date	May 2026
Prepared by	Mykolas Romeris University (MRU) - Research Team
Project	AICP-FIMI - AI-Driven Cloud Platform to Counter FIMI during Elections
Consortium Lead	UAB Acrux Cyber Services
Partners	VilniusTech; KTU; Mykolas Romeris University (MRU)
Classification	Research Report - Internal Project Document

Table of Contents

Executive Summary

This report presents the scientific research findings of Mykolas Romeris University (MRU) on personal data protection and GDPR compliance for the AICP-FIMI platform - an AI-driven cloud system designed to counter Foreign Information Manipulation and Interference (FIMI) during elections and to provide early-warning identification of social media bot and troll farm activity.

The report addresses four Lithuanian research requirements: (1) scientific research report on GDPR compliance (moksliniu tyrimu BDAR atitikties ataskaita); (2) implementing Privacy by Design and Privacy by Default; (3) identifying and managing privacy risks; and (4) conducting a Data Protection Impact Assessment (DPIA). Version 2.0 incorporates all corrections identified in the formal critical review, including two previously missing critical legal analyses - Law Enforcement Directive intersection (Section 5.9) and Article 10 GDPR (Section 5.2.3) - elevated risk scores for three categories, three new risk categories, and enhanced VDAI consultation scenario analysis.

Key Findings

The AICP-FIMI platform processes personal data of social media users including account data, content, metadata, network relationships, and behavioural patterns. NLP-based political content analysis creates a substantive risk of processing data revealing political opinions, triggering GDPR Article 9. Risk scores may constitute criminal offences data under Article 10 GDPR where FIMI operations are criminalised under Lithuanian law.

Two CRITICAL stop-ship conditions apply: (1) no confirmed legal basis for operational processing of political-content social media data at scale (Article 6 gap); (2) no confirmed Article 9(2) basis for processing political opinion data inferred by the NLP pipeline. A dedicated Lithuanian legislative mandate under Article 6(1)(e) GDPR is the recommended solution. The platform must not be operationally deployed without resolving these conditions.

DPIA screening confirms that a formal DPIA is mandatory - all nine EDPB high-risk criteria are triggered. VDAI prior consultation under Article 36 GDPR is required before deployment. The report identifies 22 compliance gaps (7 CRITICAL, 10 HIGH, 5 MEDIUM), 32 structured recommendations, and a four-phase implementation roadmap.

Key Changes in v2.0

- Section 5.9 ADDED: Law Enforcement Directive (2016/680) intersection - alert transmission to law enforcement triggers LED analysis at recipient level and requires separate GDPR legal basis.
- Section 5.2.3 ADDED: Article 10 GDPR criminal offences data - where FIMI classification data relates to suspected criminal conduct, Article 10 applies as additional legal basis requirement.
- PR-13 (Discrimination/Minority) ELEVATED TO CRITICAL (Score 20): Russian-speaking minority faces compounding NLP performance failure and political suspicion risk with electoral rights implications under ECHR Art.14 and Charter Art.21.
- PR-05 (Chilling Effect) ELEVATED TO HIGH (Score 15) based on academic evidence (Penney 2016, Stoycheff 2016). PR-14 (Vulnerable Group) ELEVATED TO HIGH (Score 15).

- Three NEW risk categories: PR-NEW-01 (Automation Bias), PR-NEW-02 (FIMI Classification Capture), PR-NEW-03 (Adversarial Evasion).
- Section 9.6.1 ADDED: VDAI Art.36 scenario analysis (Scenarios A through D).
- CG-21 and CG-22 ADDED: LED and Art.10 compliance gaps. Total now 22 gaps (7 CRITICAL).
- REC-T09 RECLASSIFIED from MANDATORY to BEST PRACTICE with proportionality justification.
- Subgroup fairness audit MOVED to Phase 1 (pre-deployment) from Phase 2.
- Section 12.4.1 ADDED: AI Act Article 5 prohibited practices assessment.
- Contextual integrity (Nissenbaum 2004/2010) added to Section 4.1.
- LI academic critique (Kosta 2013, Zanfir-Fortuna 2021) and case law added to Section 5.2.2.
- NIS2 Directive (2022/2555) assessment added to Section 5.7.
- Meta case labelling corrected to "Bundeskartellamt" (C-252/21) throughout.
- Bibliography expanded with 11 new entries.

Introduction and Research Context

1.1 Research Mandate and Objectives

This report is produced by Mykolas Romeris University (MRU) under the AICP-FIMI research project. MRU's mandate is to address the legal, ethical, and compliance dimensions of the AICP-FIMI platform. The report constitutes the primary deliverable of MRU's research assignment, addressing four specific requirements established in the project agreement.

1.2 Research Contribution

This report constitutes, to the authors' knowledge, the first comprehensive GDPR/data protection compliance framework specifically designed for an AI-driven FIMI detection and election integrity monitoring platform. While there is a growing body of literature on GDPR compliance for AI systems in general, and a nascent literature on counter-disinformation policy, the systematic application of Article 35 DPIA methodology, Article 22 automated decision-making analysis, Article 9 special-category data assessment, and fundamental rights impact analysis to AI-driven FIMI monitoring has not previously been addressed in published research.

The framework developed in this report - including the eighteen-category privacy risk taxonomy (fifteen base categories plus three new categories identified in critical review), the dual-legal-basis analysis for election-monitoring AI, and the compliance-by-design integration of Article 25 controls into an NLP-based political content analysis pipeline - constitutes an original contribution to the literature at the intersection of AI governance, election integrity law, and data protection.

1.3 The AICP-FIMI Project

The AICP-FIMI project develops an AI-driven cloud platform to counter Foreign Information Manipulation and Interference (FIMI) during elections and to provide early-warning identification of social media bot and troll farm activity. The platform aims to identify coordinated inauthentic behaviour, detect bots and troll farms, analyse account behaviour, linguistic patterns, network structures, content, sentiment and emotionality, and support real-time alerts to authorities and election monitors.

The consortium comprises four partners: UAB Acrux Cyber Services (project lead, product development, integration, real-life testing); VilniusTech (ML model development and pattern recognition); Kaunas University of Technology (NLP-based text analysis and R&D); and Mykolas Romeris University (GDPR compliance, secure processing, privacy compliance and risk management).

1.4 Research Methodology

The research methodology is grounded in legal doctrinal analysis combined with a compliance-engineering approach. Primary legal sources - GDPR, AI Act, Digital Services Act, Law Enforcement Directive, NIS2, EU Charter of Fundamental Rights, ECHR - form the foundational layer. CJEU and ECtHR case law provides interpretive authority. EDPB and VDAI supervisory guidance provides regulatory interpretation. ISO/IEC standards and ENISA guidance provide technical compliance context.

The DPIA methodology follows EDPB Guidelines WP248 rev.01. The privacy risk taxonomy employs a 5x5 likelihood-impact matrix consistent with ISO/IEC 27005 risk management principles. Recommendations are

classified as MANDATORY (legal requirement), BEST PRACTICE (strongly recommended), or ADVISORY (project-specific recommendation). Version 2.0 incorporates all corrections from the formal critical review (AICP-MRU-CRITICAL-REVIEW-RESULTS-v1.0), conducted using a multi-role adversarial methodology across VDAI examiner, civil society, academic, and defence counsel perspectives.

CHAPTER 2

AICP-FIMI System and Technical Context

2.1 System Overview

The AICP-FIMI platform is an AI-driven analytical system that collects and processes social media data to identify potential FIMI activity, particularly during election periods. The platform combines: (a) social media data collection (public posts, account metadata, interaction networks); (b) Natural Language Processing (NLP) for text and sentiment analysis; (c) network analysis for coordinated behaviour detection; (d) behavioural pattern analysis and anomaly detection; (e) machine learning classification models; (f) risk scoring and alert generation; and (g) reporting and dashboard interfaces for operators.

2.2 Privacy-Relevant Processing Operations

From a data protection perspective, the following processing operations are privacy-relevant: (1) collection of account-level data including usernames, profile information, and posting history; (2) content data collection including posts, replies, shares, and linguistic features; (3) metadata collection including timestamps, engagement metrics, and technical identifiers; (4) inference operations generating features from content analysis including sentiment, emotionality, political orientation signals, and linguistic provenance; (5) network analysis linking individual accounts through interaction patterns; (6) risk score assignment to individual accounts; (7) alert generation flagging specific accounts as suspected FIMI actors; and (8) transmission of alerts and reports to operators, clients, and potentially law enforcement authorities.

Each of these operations involves personal data - social media accounts belong to identifiable natural persons, even where pseudonymous usernames are used. The inference operations create new personal data (risk scores, FIMI classifications) that did not previously exist and are subject to the full GDPR framework.

2.3 Deployment Context and Election-Period Activation

The platform is designed for deployment in connection with election periods, with heightened monitoring intensity during the pre-election and election-day windows. This election-period context is significant for compliance analysis: (a) election-period data subjects include politically active individuals whose participation rights under ECHR Protocol 1 Article 3 and EU Charter Article 39 are directly engaged; (b) election-period data inherently includes political content triggering Article 9 GDPR; (c) the stakes of erroneous FIMI classification are highest during elections, when false positives affect individuals' exercise of electoral rights; and (d) election-period monitoring by a private entity operating on behalf of state-adjacent authorities raises heightened proportionality concerns under ECHR Article 8.

CHAPTER 3

Research Scope and Regulatory Framework

3.1 Primary EU Legal Instruments

The primary regulatory framework for AICP-FIMI compliance analysis comprises the following EU legal instruments: Regulation (EU) 2016/679 (GDPR/BDAR) - the foundational instrument governing all personal data processing; Directive (EU) 2016/680 (Law Enforcement Directive, LED) - governing downstream processing by law enforcement authorities of AICP-FIMI alert data; Regulation (EU) 2024/1689 (AI Act) - classifying and regulating AI systems including political content analysis tools; Regulation (EU) 2022/2065 (Digital Services Act, DSA) - governing platform obligations relevant to FIMI-related content; Directive (EU) 2022/2555 (NIS2) - cybersecurity requirements applicable to managed security service providers; and the EU Charter of Fundamental Rights.

3.2 Council of Europe Instruments

The European Convention on Human Rights (ECHR) - Articles 8 (private life), 10 (expression), 14 (non-discrimination), and Protocol 1 Article 3 (free elections) - provides the fundamental rights framework. Convention 108+ (Council of Europe Convention on Automated Processing of Personal Data, modernised) provides additional data protection standards relevant to automated profiling. ECtHR case law on surveillance, profiling, and political expression is analysed in Chapter 12.

3.3 Lithuanian Law and VDAI Guidance

Lithuanian national law implementing GDPR is primarily the Law on Legal Protection of Personal Data (Asmens duomenu teisines apsaugos istatymas). The State Data Protection Inspectorate (Valstybine duomenu apsaugos inspekcija, VDAI) is the competent supervisory authority. The specific question of whether Lithuanian law provides a sufficient legislative basis for election-period FIMI monitoring under Article 6(1)(e) GDPR is a central unresolved compliance question addressed in Chapter 5.

3.4 AI Act Classification

Under the AI Act, AICP-FIMI likely qualifies as a high-risk AI system under Annex III, particularly under category 8 (AI systems intended to detect deep fakes) and potentially under category 6 (law enforcement AI systems if deployed in that context). High-risk AI system status triggers conformity assessment, transparency requirements, human oversight obligations, accuracy and robustness requirements, and registration obligations. Chapter 12 analyses the AI Act intersection in detail, including an Article 5 prohibited practices assessment (Section 12.4.1) and a Fundamental Rights Impact Assessment (FRIA) vs DPIA distinction analysis.

CHAPTER 4

Personal Data and Data Flow Inventory

4.1 Scope of Personal Data Processing

The AICP-FIMI platform collects and processes data relating to identified and identifiable natural persons within the meaning of Article 4(1) GDPR. Social media account identifiers - whether real names, pseudonymous usernames, or numerical user IDs - are personal data because they can be linked to identifiable individuals directly or indirectly, particularly in combination with IP addresses, device identifiers, posting patterns, and linguistic fingerprints. The Court of Justice of the European Union confirmed in Breyer (C-582/14) that online pseudonymous identifiers constitute personal data where re-identification is reasonably possible.

The collection of public social media data does not negate GDPR applicability. The GDPR applies to any processing of personal data "wholly or partly by automated means" regardless of whether the data was publicly accessible at source. The EDPB has consistently confirmed that web scraping and automated collection of public social media content constitutes processing of personal data subject to full GDPR compliance obligations (EDPB Letter to MEPs on Facebook scraping, 2021; EDPB Guidelines 8/2020 on targeting social media users).

> Contextual Integrity and Public Social Media Data (Nissenbaum): The scope of personal data protection for public social media content is illuminated by Nissenbaum's theory of contextual integrity (Nissenbaum, 2004, Privacy as Contextual Integrity, Washington Law Review 79(1), 119-158; Nissenbaum, 2010, Privacy in Context). According to this theory, information flows are appropriate when they match the norms of the context in which information was originally shared. A user who posts political commentary on a public Twitter/X account does so within the norms of public political discourse - norms that include being read, quoted, and responded to by other participants, but not systematic automated aggregation, behavioural profiling, and risk scoring by a security monitoring system. Even where information is technically "public", its appropriation for a context (security surveillance) that violates the norms of the original context constitutes a privacy violation in the contextual integrity sense. The CJEU's holding in Latvijas Padomju (C-439/19) that systematic publication of political activity data engages Article 9 GDPR even where that data was previously accessible reflects a legally operative version of the contextual integrity intuition: context matters for the lawfulness of data use, not merely accessibility.

4.2 Data Categories

The following categories of personal data are collected or generated by the AICP-FIMI platform:

ID	Category	Examples	Source	GDPR Risk
DC-01	Account Identifiers	Username, user ID, display name, profile URL, account creation date	Social media APIs / scraping	Standard personal data
DC-02	Profile Data	Profile description, location, follower count, following count, profile image	Social media APIs / scraping	Standard personal data
DC-03	Content Data	Posts, comments, replies, retweets, shares, hashtags, mentions	Social media APIs / scraping	May include Art.9 data

DC-04	Metadata	Timestamps, geographic location metadata, device type, language setting	Social media APIs	Location data sensitive
DC-05	Network Data	Follower/following relationships, interaction patterns, group memberships	Social media APIs / network analysis	Reveals associations
DC-06	Behavioural Data	Posting frequency, activity patterns, temporal behaviour, engagement metrics	Derived / computed	Profiling - Art.22
DC-07	Linguistic Features	Language, writing style, syntactic patterns, NLP-extracted features	NLP pipeline	May reveal origin/identity
DC-08	Sentiment / Emotionality	Sentiment polarity, emotionality scores, toxicity scores	NLP inference	Inferred data - Art.9 risk
DC-09	Political Content Features	Political topic signals, narrative alignment, ideological indicators	NLP inference	Art.9(1) political opinions risk
DC-10	Network Graph Features	Centrality scores, community membership, coordination indices	Network analysis	Reveals associations
DC-11	Risk Scores	Bot probability score, FIMI risk score, troll farm classification	ML model output	New inferred personal data
DC-12	Training / Validation Data	Labelled datasets used for model training	Dataset compilation	Depends on source

4.3 Data Lifecycle

The AICP-FIMI data lifecycle comprises seven stages, each with distinct processing operations, data flows, and compliance obligations:

Stage	Operations	Personal Data Involved	Compliance Trigger
1. Collection	API queries, web scraping, data ingestion	DC-01 to DC-05	Legal basis; data minimisation; transparency
2. Processing	Cleaning, deduplication, normalisation, annotation	DC-01 to DC-08	Purpose limitation; accuracy
3. Analysis	NLP analysis, network analysis, feature extraction	DC-07 to DC-11	Art.9 risk; automated processing Art.22
4. Model Training	ML training on labelled datasets	DC-12	Separate processing purpose; storage limitation
5. Classification	Risk score assignment, alert generation	DC-11	Art.22; profiling safeguards; accuracy
6. Reporting	Alert transmission, dashboard display, reports to clients	DC-01, DC-11	Controller/processor split; LED intersection
7. Retention/Deletion	Data archiving, deletion per retention schedule	All categories	Storage limitation; secure deletion

CHAPTER 5

GDPR Compliance Analysis

5.1 Article 5 - Data Processing Principles

Article 5 GDPR establishes the foundational principles governing all personal data processing. Each principle is assessed against the AICP-FIMI processing operations.

Principle (Art.5)	Requirement	AICP-FIMI Application	Compliance Status
Lawfulness, Fairness, Transparency (5(1)(a))	Legal basis required; processing must be fair and transparent to data subjects	Legal basis gap identified (see Section 5.2); transparency to monitored users absent in current design	CRITICAL GAP
Purpose Limitation (5(1)(b))	Data collected for specified purposes; not further processed incompatibly	FIMI monitoring purpose defined; training datasets must be scoped; law enforcement transmission may be incompatible purpose	PARTIAL GAP
Data Minimisation (5(1)(c))	Adequate, relevant, limited to what necessary	Large-scale collection of all public posts; minimisation controls required	REQUIRES CONTROLS
Accuracy (5(1)(d))	Personal data accurate and kept up to date; inaccurate data erased	False positive risk from ML model; no automated correction mechanism in current design	GAP
Storage Limitation (5(1)(e))	Data not kept longer than necessary for purposes	Retention policy not defined in current design	GAP
Integrity and Confidentiality (5(1)(f))	Appropriate security to protect against unauthorised access, loss, destruction	Security controls to be assessed per Art.32; encryption and access control required	REQUIRES IMPLEMENTATION
Accountability (5(2))	Controller responsible for compliance and able to demonstrate it	DPO appointment; Art.30 records; DPIA required; documentation framework needed	REQUIRES IMPLEMENTATION

5.2 Article 6 - Legal Bases for Processing

5.2.1 Assessment of Available Legal Bases

The identification of a valid legal basis under Article 6(1) GDPR is a prerequisite for lawful processing. The following legal bases are assessed for AICP-FIMI:

Article 6(1)(a) - Consent: Not available for AICP-FIMI. Consent requires freely given, specific, informed, and unambiguous indication by the data subject. Covert monitoring of social media users without their knowledge is structurally incompatible with consent as a legal basis.

Article 6(1)(e) - Public Task: Available in principle for controllers performing tasks in the public interest or in the exercise of official authority. AICP-FIMI serves the public interest in election integrity and democratic resilience. However, Article 6(1)(e) requires that the task be laid down in Union or Member State law. No current Lithuanian legislative instrument explicitly authorises private-sector AI-driven FIMI monitoring at election scale. This is the primary legal basis gap (CG-01).

CRITICAL COMPLIANCE GAP: CRITICAL GAP CG-01: No Lithuanian legislative instrument currently provides a clear Article 6(1)(e) legal basis for the AICP-FIMI processing operations. The consortium must engage with the Lithuanian Parliament and Government to seek enactment of dedicated FIMI monitoring legislation before operational deployment. Without this basis, operational processing constitutes a GDPR violation.

Article 6(1)(f) - Legitimate Interest: Available as a potential provisional basis during the research and development phase. The three-part test - legitimate interest pursued, necessity of processing, no override by data subjects' interests - is analysed in Section 5.2.2. Legitimate interest is not a viable long-term basis for large-scale election-period political content monitoring.

5.2.2 Legitimate Interest Assessment

The GDPR Article 6(1)(f) legitimate interest basis requires satisfaction of a three-part test: (1) there is a legitimate interest; (2) processing is necessary for that interest; and (3) the interest does not override the data subjects' fundamental rights and freedoms. The CJEU developed this framework in Rigas (C-13/16, ECLI:EU:C:2017:336), and EDPB Guidelines 1/2024 on legitimate interest provide the current authoritative interpretation.

The three-part LI test has been developed across a line of CJEU authorities: Tietosuojavaltuutettu v Satakunnan Markkinaporssi Oy and Satamedia Oy (C-73/07, ECLI:EU:C:2008:727); Article 29 Working Party Opinion 6/2014 on the Notion of Legitimate Interests; ASNEF and FECEMD (Joined Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777); and most recently Orange Romania (C-61/19, ECLI:EU:C:2020:901) confirming that the necessity and balancing elements must be rigorously assessed.

Step 1 - Legitimate Interest: The interest in protecting democratic processes from foreign information manipulation is legitimate. Election integrity is a recognised public interest, and the CJEU has confirmed that private sector actors can pursue public interest goals as a legitimate interest where they are genuine and lawful.

Step 2 - Necessity: Processing social media account data for FIMI detection is necessary for the stated interest, subject to the principle that no less intrusive means exist to achieve the same objective. Necessity is satisfied for the R&D phase; it is more questionable at operational election scale.

Step 3 - Balancing: The balancing of interests weighs the data controller's legitimate interest against the data subjects' rights and freedoms. In the election context, this balance is heavily affected by: (a) the political sensitivity of the data; (b) the risk of false positive classification affecting electoral participation; (c) the covert nature of the monitoring (no notice to monitored individuals); and (d) the scale of processing during election periods. The balance is tenuous, particularly for politically active individuals.

Academic Critique of LI for Covert Political Monitoring: The academic literature on legitimate interest raises a structural objection to its use for covert, large-scale monitoring of political expression by private actors. Kosta (2013) and Zanfir-Fortuna (2021) argue that the balancing test in the third step of the LI analysis cannot be meaningfully conducted where data subjects are unaware of the processing and cannot exercise the Article 21 override right in practice - the theoretical availability of the right to object is illusory where the data subject does not know they are being profiled. This structural critique is particularly relevant to AICP-FIMI. The present analysis concludes that LI is available as a provisional basis pending legislative mandate, but acknowledges the force of this critique: LI is inherently fragile for AICP-FIMI-type processing and should not be treated as a long-term compliance solution. The consortium's priority must be establishing the Article 6(1)(e) legislative mandate, with LI serving only as an interim basis during the research and development phase.

5.2.3 Article 10 GDPR - Criminal Convictions and Offences Data [NEW v2.0]

Article 10 GDPR provides that processing of personal data relating to criminal convictions and offences may be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. The CJEU has interpreted Article 10 broadly: it applies not only to data about confirmed convictions but also to data that implies the commission of a criminal offence.

Application to AICP-FIMI: In several EU Member States including Lithuania, foreign information manipulation may constitute a criminal offence under national law. Where AICP-FIMI risk scores are used to identify individuals suspected of operating FIMI campaigns constituting criminal offences, the data processed and the risk scores generated may constitute data relating to criminal offences within the meaning of Article 10. The consequence of Article 10 applying is that Acrux as controller cannot rely solely on Article 6(1)(e) or (f) as the legal basis for processing - a specific legislative authorisation providing appropriate safeguards is required.

CRITICAL COMPLIANCE GAP: ADDITIONAL STOP-SHIP CONDITION (CG-22): If AICP-FIMI risk scores and alerts are understood as data relating to suspected criminal conduct (FIMI offences), Article 10 GDPR applies in addition to the Article 9 restriction. No private-sector entity may process such data without explicit legislative authorisation providing appropriate safeguards. This analysis should be included in the formal legal opinion recommended under REC-L01 and confirmed before any operational processing.

5.3 Article 9 - Special Category Data: Political Opinions

CRITICAL COMPLIANCE GAP: CRITICAL GAP CG-02: NLP-based political content analysis by the AICP-FIMI platform is likely to process data revealing political opinions within the meaning of Article 9(1) GDPR. Processing of special category data is prohibited unless one of the exhaustive exceptions in Article 9(2) applies. No applicable Article 9(2) basis has been identified for the AICP-FIMI operational processing. This is a CRITICAL stop-ship condition.

Article 9(1) prohibits the processing of personal data revealing political opinions. The CJEU has confirmed in Latvijas Padomju (C-439/19) that data which reveals political activity or associations of individuals constitutes special category data even where that data was previously accessible to the public. The NLP pipeline's analysis of political content for FIMI detection necessarily involves processing data that reveals political opinions - the very objective of identifying politically motivated foreign manipulation requires analysis of political content and classification of political stance.

Available Article 9(2) bases assessed: Art.9(2)(g) (substantial public interest) requires Union or Member State law providing for suitable safeguards - same legislative gap as Article 6(1)(e). Art.9(2)(d) (legitimate activities of non-profit bodies with political aims) does not apply to a commercial cybersecurity company. Art.9(2)(e) (manifestly made public) is inapplicable - data made public for one purpose does not become available for all purposes per Latvijas Padomju. The Article 9 gap is confirmed.

5.4 Article 22 - Automated Decision-Making and Profiling

Article 22(1) GDPR provides that data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects concerning them. The AICP-FIMI risk score assignment and FIMI classification constitute profiling within the meaning of

Article 4(4) GDPR - the automated analysis of personal data to evaluate, analyse, or predict aspects of natural persons including their behaviour, interests, and location.

The SCHUFA judgment (C-634/21, ECLI:EU:C:2023:957) significantly expanded the scope of Article 22: the CJEU held that an automated creditworthiness score constituted an Article 22 decision where it "determines in a decisive manner" the human decision that follows. Applied to AICP-FIMI: where analysts routinely follow automated risk scores without genuine independent review - a pattern facilitated by automation bias - the automated component effectively "determines in a decisive manner" the downstream alert decision, engaging Article 22 regardless of the nominal human review step. Article 22(2) exceptions require explicit consent or legal authorisation - again subject to the legislative gap.

5.5 Articles 12–22 - Data Subject Rights

AICP-FIMI data subjects retain all rights under Chapter III GDPR notwithstanding the public/covert nature of monitoring. Key rights analysis:

Right	Art.	Challenge for AICP-FIMI	Required Action
Transparency	13/14	Covert monitoring means Art.14 notice obligation applies; privacy notice to be published for public social media monitoring	Publish Art.14 privacy notice before deployment
Access	15	Data subjects can request copy of all data held; risk score and classification must be disclosed	Implement SAR handling procedure
Rectification	16	Right to correct inaccurate risk scores; false positive mechanism required	Implement correction mechanism with DPO oversight
Erasure	17	Right to erasure where processing unlawful or data no longer necessary	Implement deletion pipeline; document retention justifications
Restriction	18	Right to restrict processing during accuracy disputes	Implement processing suspension mechanism
Portability	20	Applies to consent and contract bases; not to LI or public task	Not applicable on current legal basis
Objection	21	Right to object to LI processing; objection must be honoured unless compelling legitimate grounds	Implement objection handling; Art.21 notice in privacy notice
No automated decisions	22	Profiling safeguards; human review genuine not nominal	Genuine human oversight; SCHUFA-compliant review process

5.6 Article 30 Records and Article 32 Security

Article 30 GDPR requires the controller to maintain a record of processing activities. For AICP-FIMI, the Article 30 record must document: each processing operation (collection, NLP analysis, network analysis, risk scoring, alerting, transmission); purpose; categories of data; categories of recipients (including law enforcement authorities where alerts are transmitted); retention periods; and security measures. The record must be updated when new processing operations are added, including each model retraining cycle.

Article 32 GDPR requires implementation of appropriate technical and organisational security measures. For AICP-FIMI, minimum security requirements include: encryption of personal data at rest and in transit; access controls with role-based permissions; pseudonymisation of account identifiers in non-production environments; audit logging; incident response procedures; and regular security testing.

5.7 Article 32 Security and NIS2 Assessment [UPDATED v2.0]

The technical and organisational security measures required under Article 32 GDPR must be appropriate to the risk level. For AICP-FIMI, with its processing of political opinion data and election-period risk context, a high security standard is required. Controls include: end-to-end encryption; zero-trust access architecture; penetration testing before deployment; vulnerability management programme; and secure deletion mechanisms with cryptographic erasure verification.

NIS2 Directive Assessment (Article 21 NIS2): Directive (EU) 2022/2555 (NIS2) requires entities qualifying as "essential" or "important" entities to implement cybersecurity risk management measures and report significant incidents to the national CSIRT. UAB Acrux Cyber Services should assess whether AICP-FIMI qualifies under NIS2 Annex II as a managed security service provider supporting critical infrastructure (election integrity systems). If NIS2 applies: (a) cybersecurity risk management requirements under Article 21 NIS2 apply in addition to Article 32 GDPR - substantial overlap exists but NIS2 includes additional requirements (supply chain security, vulnerability handling policies); (b) significant security incidents must be reported to the Lithuanian National Cyber Security Centre (NKSC) within 24 hours (early warning) and 72 hours (incident notification) under Article 23 NIS2; (c) the NIS2 incident notification obligation is in addition to the GDPR Article 33 breach notification obligation to the VDAI. The NIS2 qualification assessment should be conducted by Acrux legal counsel and documented before deployment.

5.8 International Data Transfers

Where personal data is processed by cloud infrastructure providers outside the EEA, or where technical partners are established outside the EEA, GDPR Chapter V applies. Transfers to third countries require either an adequacy decision (Article 45), standard contractual clauses with a Transfer Impact Assessment (TIA) following Schrems II (C-311/18), or another Chapter V mechanism. The consortium must map all data flows to third countries and confirm that valid transfer mechanisms are in place for each. Cloud provider contracts must include Article 28 data processing agreements and confirm EU/EEA data residency where possible.

5.9 Law Enforcement Directive (LED) Intersection [NEW v2.0]

Where AICP-FIMI alerts are transmitted to law enforcement authorities - including the Lithuanian Police, the Prosecutor's Office, or the State Security Department - those recipients process the transmitted personal data for law enforcement purposes. Directive (EU) 2016/680 (the Law Enforcement Directive, LED) applies to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties. Accordingly, the LED governs the downstream processing of AICP-FIMI alert data by law enforcement recipients; GDPR continues to govern Acrux's own processing as the alert-transmitting controller.

Implications for the transmitting controller (Acrux): The transmission of personal data to a law enforcement authority constitutes a disclosure to a third party requiring a valid Article 6 GDPR legal basis and, where special-category data is included in the alert, an Article 9(2) basis for the disclosure. The existence of the LED as the governing framework for the recipient does not provide a legal basis for the transmitting controller's disclosure - the transmitting controller must separately justify the disclosure under GDPR Chapter II. Applicable bases for law enforcement disclosure may include Article 6(1)(c) (legal obligation) where Lithuanian law requires disclosure of FIMI evidence to law enforcement, or Article 6(1)(e) (public task) where the disclosure is part of a statutorily mandated FIMI monitoring function.

Article 10 LED implications: Article 10 LED (analogous to Article 9 GDPR) prohibits the processing of special categories of personal data - including data revealing political opinions - by law enforcement authorities unless strictly necessary and subject to appropriate safeguards provided by EU or Member State law. Where AICP-FIMI alerts include or imply political opinion data, the law enforcement recipient must have

a specific LED Article 10 basis for processing that data. The consortium should assess, for each intended law enforcement recipient, whether such a basis exists under Lithuanian law.

CRITICAL COMPLIANCE GAP: COMPLIANCE ACTION REQUIRED (CG-21): Before any AICP-FIMI alert is transmitted to a law enforcement authority, the legal basis for that specific disclosure must be assessed under both GDPR Chapter II (Acrux as transmitting controller) and LED Article 10 (recipient as law enforcement authority). Where the LED analysis cannot confirm an adequate basis, alerts to law enforcement must be suspended pending legal basis confirmation. This requirement must be documented as a separate item in the Article 30 record of processing activities. See also Chapter 6 (Controller/Processor analysis, Section 6.2) for joint controller implications where law enforcement authorities co-define alert criteria.

Compliance Gap Summary - Chapter 5:

Gap ID	Severity	Description	Required Action
CG-01	CRITICAL	No Art.6(1)(e) legislative basis for FIMI monitoring	Seek Lithuanian legislative mandate before deployment
CG-02	CRITICAL	No Art.9(2) basis for political opinion data processing	Legislative basis or halt NLP political content analysis
CG-03	CRITICAL	No Art.14 transparency notice published for monitored users	Publish GDPR Art.14 privacy notice before any data collection
CG-04	HIGH	Art.22 profiling safeguards not implemented	Implement genuine human oversight and SCHUFA-compliant review
CG-05	HIGH	Data retention schedule not defined	Establish retention policy with documented justifications
CG-21	CRITICAL	LED intersection not assessed for law enforcement alert recipients	Conduct LED applicability assessment before transmitting alerts
CG-22	CRITICAL	Art.10 GDPR criminal offences data assessment absent	Commission formal legal opinion on Art.10 applicability

CHAPTER 6

Controller and Processor Role Analysis

6.1 Framework: Controller, Joint Controller, Processor

Article 4(7) GDPR defines the controller as the natural or legal person which alone or jointly with others determines the purposes and means of processing. Article 4(8) defines the processor as a natural or legal person which processes personal data on behalf of the controller. Article 26 governs joint controllers - where two or more controllers jointly determine the purposes and means of processing, they are joint controllers and must agree the allocation of compliance responsibilities in a transparent arrangement.

The correct identification of controller, joint controller, and processor roles is fundamental to AICP-FIMI compliance: it determines which entity bears each compliance obligation, which must conduct the DPIA, which must respond to data subject requests, and which must notify the VDAI in the event of a data breach.

6.2 Controller/Processor Role Matrix

Entity	Primary Role	Processing Activities	Joint Controller Scenarios	Legal Instrument
UAB Acrux Cyber Services	Primary Controller	Platform design, data collection, ML pipeline, alert generation, client reporting	Joint controller with law enforcement where alert criteria co-defined (Art.26)	Internal privacy policy; DPA agreements; Art.26 arrangement with law enforcement
VilniusTech	Processor / Joint Controller (R&D)	ML model development using Acrux-provided training data	Possible joint controller where VilniusTech determines feature design that affects processing purposes	Art.28 DPA; potential Art.26 arrangement
KTU	Processor / Joint Controller (R&D)	NLP pipeline development using Acrux-provided datasets	Possible joint controller for NLP design decisions	Art.28 DPA; potential Art.26 arrangement
MRU	Independent Controller (Research)	GDPR compliance research; no operational data processing	Not a controller for operational AICP-FIMI processing	Research ethics framework; own Art.30 records
Cloud Provider(s)	Processor	Infrastructure, storage, compute	Processor only - does not determine purposes	Art.28 DPA with data residency clauses
Law Enforcement Recipients	Independent Controller under LED	Processing of transmitted alert data for law enforcement purposes	Possible joint controller where alert criteria co-defined (Art.26 GDPR + Art.10 LED)	Art.26 arrangement; LED compliance framework
Client Organizations	Controller / Joint Controller	Receipt and use of AICP-FIMI alerts and reports	Joint controller where client configures alert thresholds or monitoring targets	Art.26 arrangement defining respective responsibilities

6.3 Joint Controller Obligations - Article 26 GDPR

Where joint controllership exists, Article 26(1) GDPR requires that the joint controllers determine in a transparent manner and by means of an arrangement their respective responsibilities for compliance with the GDPR obligations. The arrangement must reflect their actual roles and relationships and must be made available to data subjects on request (Article 26(2)). The CJEU confirmed in Wirtschaftsakademie (C-210/16) and Fashion ID (C-40/17) that any entity that participates in determining the purposes and means of processing is a joint controller, regardless of its formal contractual status.

Required Article 26 arrangements for AICP-FIMI: (1) Acrux + Law Enforcement: where Lithuanian law enforcement authorities define alert criteria and threshold settings that influence what personal data is collected and how it is classified, they jointly determine the means of processing with Acrux. An Article 26 arrangement must define which entity is responsible for Article 30 records, DPIA, data subject rights responses, and breach notification. (2) Acrux + Client Organizations: where clients configure monitoring parameters, similar joint controllership may arise requiring an Article 26 arrangement.

6.4 Article 28 Processor Agreements

Article 28 GDPR requires that processing by a processor be governed by a binding contract setting out the subject matter, duration, nature and purpose of processing, the type of personal data, the categories of data subjects, and the obligations and rights of the controller. Article 28(3) specifies the mandatory content of processor agreements. For AICP-FIMI, Article 28 agreements are required between: Acrux and VilniusTech; Acrux and KTU; Acrux and cloud infrastructure providers; and Acrux and any subprocessors (monitoring tool vendors, API providers). All agreements must include the Article 28(3)(h) requirement to assist the controller in ensuring compliance with security, breach notification, DPIA, and prior consultation obligations.

6.5 DPO Appointment Requirement

Article 37 GDPR requires appointment of a Data Protection Officer where processing is carried out on a large scale and involves special category data (Article 37(1)(b)), or where the core activities involve large scale, regular and systematic monitoring of individuals (Article 37(1)(c)). AICP-FIMI triggers both conditions: it involves large-scale election-period monitoring of social media users and processes political opinion data. DPO appointment by Acrux (as primary controller) is mandatory. Where VilniusTech or KTU engage in large-scale processing of personal data as part of the project, they may individually require DPO appointments under their own applicable thresholds.

CHAPTER 7

Privacy by Design and Privacy by Default

7.1 Article 25 GDPR - Legal Requirement

Article 25 GDPR establishes the legal obligation to implement Privacy by Design and Privacy by Default. Article 25(1) requires the controller, both at the time of determining the means for processing and at the time of processing itself, to implement appropriate technical and organisational measures designed to implement data protection principles effectively and to integrate the necessary safeguards into the processing. Article 25(2) requires the controller to implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose are processed.

The EDPB Guidelines 4/2019 on Article 25 Privacy by Design and by Default identify eight data protection goals that privacy engineering must address: data minimisation; purpose limitation; storage limitation; accuracy; confidentiality; integrity; availability; and transparency/accountability. Each goal is operationalised through specific technical and organisational measures.

7.2 Privacy by Design - Control Framework

7.2.1 Data Minimisation (PBD-01)

Only personal data strictly necessary for the FIMI detection purpose should be collected and retained. This requires: (a) field-level minimisation at collection - excluding data fields not required for analysis (e.g., precise GPS coordinates, email addresses, phone numbers); (b) time-window minimisation - collecting only data from the relevant monitoring period rather than full historical account data; (c) threshold-based collection - collecting detailed data only for accounts meeting initial risk threshold criteria, not all accounts in a monitored network; and (d) training data minimisation - using synthetic data augmentation where real personal data can be substituted.

7.2.2 Pseudonymisation (PBD-02)

Article 25(1) specifically refers to pseudonymisation as an appropriate technical measure. For AICP-FIMI: (a) account identifiers should be pseudonymised in all non-production environments (development, testing, research) - replacing real usernames and user IDs with synthetic identifiers; (b) the pseudonymisation key should be held separately with access restricted to the DPO and operational security team; (c) pseudonymisation should be reversed only when an alert reaches the threshold requiring human review and potential transmission - at which point de-identification is no longer appropriate; and (d) training datasets used by VilniusTech and KTU should use pseudonymised or synthetic data wherever technically feasible.

7.2.3 Access Controls and Role-Based Permissions (PBD-03)

Access to personal data should be restricted to authorised roles with a documented need-to-access: (a) Data Collection Layer - system processes only, no human access; (b) Analysis Layer - ML/NLP engineers access pseudonymised data for model development; (c) Alert Review Layer - trained analysts access de-pseudonymised data for flagged accounts above threshold only; (d) Reporting Layer - authorised clients access aggregated reports and specific alerts (not underlying raw data); (e) DPO/Security - access to all layers

for compliance monitoring. Access permissions should be reviewed quarterly and revoked immediately on role change.

7.2.4 Secure Architecture and Encryption (PBD-04)

Technical security controls required by Privacy by Design: (a) encryption of all personal data at rest using AES-256 or equivalent; (b) TLS 1.3 for all data in transit; (c) database-level encryption with separate key management; (d) encrypted audit logs with tamper-evident signing; (e) hardware security modules (HSM) for cryptographic key management; and (f) secure deletion using cryptographic erasure to support the right to erasure.

7.2.5 Purpose-Bound Processing and Technical Barriers (PBD-05)

Technical controls to enforce purpose limitation: (a) data governance tags at field level specifying permitted processing purposes - collected for FIMI detection cannot be used for commercial profiling; (b) automated purpose enforcement in the data processing pipeline - API access restricted by purpose; (c) technical barriers preventing export of raw personal data outside the AICP-FIMI system; (d) separate data stores for training datasets vs. operational analysis data; and (e) audit trails recording each processing operation with purpose annotation.

7.2.6 Human Review Gate (PBD-06)

A genuine human review gate is required before any alert is transmitted to a client or law enforcement authority. Genuineness requires: (a) the reviewer must have the time, information, and authority to override the automated classification; (b) the review interface must present the specific model features contributing to the risk score, not merely the score summary; and (c) the reviewer must be able to reject, modify, or escalate the alert.

> Human Review Quality Assurance - Automation Bias Mitigation: The effectiveness of the human review gate depends on genuine independent analyst judgment. Academic research on automation bias (Goddard et al., 2012; Cummings, 2014) consistently demonstrates that human reviewers of automated AI outputs tend to confirm rather than override AI recommendations - particularly under time pressure. This risk is elevated in an alert-processing context where analysts may review large volumes of alerts during election periods. To mitigate automation bias: (a) Implement a structured review interface that requires affirmative engagement with the top-5 model features contributing to the risk score before the analyst can submit a CONFIRM disposition - the analyst must acknowledge each feature; (b) Conduct a quarterly blind audit of 10% of REJECTED alerts by a senior analyst to measure the false rejection rate and identify systematic patterns; (c) Include automation bias awareness as a mandatory component of analyst training; (d) Monitor the CONFIRM rate per analyst - consistently high CONFIRM rates (>90%) should trigger a review of that analyst's review process.

7.2.7 Audit Logging and Accountability (PBD-07)

A comprehensive audit logging system is required: (a) all data access events logged with user ID, timestamp, data category accessed, and purpose annotation; (b) all alert decisions (CONFIRM/REJECT/ESCALATE) logged with reviewer ID, time taken, and key features reviewed; (c) all external transmissions (to clients, law enforcement) logged with recipient, content scope, and authorisation reference; (d) audit logs must be retained for a minimum period consistent with accountability obligations and potential legal challenges; and (e) audit log integrity protected by tamper-evident signing.

7.2.8 Data Lifecycle and Retention Controls (PBD-08)

Retention periods must be defined and technically enforced: (a) raw social media data collected during the monitoring window - maximum 12 months unless specifically justified for legal or investigative purposes; (b) alert records and classifications - minimum 24 months to support accuracy challenges and judicial review;

(c) audit logs - minimum 36 months for accountability; (d) training datasets - data minimisation review at each model retraining cycle; and (e) automated deletion mechanisms with DPO confirmation before execution.

7.3 Privacy by Default - Settings Matrix

Article 25(2) requires that by default only the minimum necessary data is processed. Privacy by Default settings for AICP-FIMI:

Setting	Default State	Override Condition	Technical Implementation
PBD-D01: Data Collection Scope	Minimum fields only (account ID, post text, timestamp)	Expanded collection requires DPO approval and documented justification	Field allowlist at API query level
PBD-D02: Analysis Depth	Network-level analysis only; no individual-level political content features active	Individual-level NLP analysis activates only for accounts exceeding network anomaly threshold	Tiered processing pipeline with threshold gate
PBD-D03: Alert Threshold	Highest precision setting (lowest false positive rate)	Lowered threshold for confirmed election emergency period requires DPO and Security Director authorisation	Threshold configuration with two-person approval
PBD-D04: Data Retention	Shortest retention period (30 days post-monitoring window)	Extended retention requires documented legal basis	Automated deletion with DPO override log
PBD-D05: Access Scope	Read-only access to aggregated data for all roles	Individual account access requires alert-specific authorisation	Role-based access control matrix
PBD-D06: External Sharing	No automatic sharing; manual DPO-approved transmission	Automated sharing to pre-approved clients requires DPO configuration approval	Transmission requires DPO digital sign-off
PBD-D07: Political Opinion Features	Political opinion classification features disabled by default	Activation requires confirmed Art.9(2) legal basis and DPO authorisation	Feature flag controlled by DPO
PBD-D08: Cross-border Transfer	EEA data residency enforced by default	Transfer outside EEA requires transfer mechanism confirmation and DPO approval	Cloud provider configuration with geographic restriction

CRITICAL COMPLIANCE GAP: IMPORTANT LIMITATION - Political Opinion Feature Gate (PBD-D07): The political opinion feature gate is a risk reduction measure, not a complete compliance solution for the Article 9 gap. NLP models trained on political content develop latent representations of political orientation that cannot be fully disabled by gating explicit output features. The gate addresses the disclosure of explicit political opinion labels; it does not prevent the model from implicitly using political orientation as a classification signal. A confirmed Article 9(2) legal basis is required regardless of whether this gate is implemented. This mitigation therefore reduces but does not eliminate Article 9 exposure, and should not be treated as a substitute for the legislative basis required under Section 5.2.1.

7.4 Implementation Checklist - Article 25 Controls

- Appoint DPO before any personal data collection commences
- Conduct Privacy by Design review of all system components (ML pipeline, NLP pipeline, alert system, dashboard)
- Implement field-level data minimisation at API collection layer
- Implement pseudonymisation for all non-production environments

- Deploy role-based access control with least-privilege defaults
- Implement AES-256 encryption at rest and TLS 1.3 in transit
- Configure purpose-bound processing with data governance tags
- Implement genuine human review gate with automation bias safeguards
- Deploy comprehensive audit logging with tamper-evident signing
- Define and technically enforce retention periods per data category
- Configure Privacy by Default settings for all eight PBD-D dimensions
- Implement political opinion feature gate with DPO-controlled activation
- Document all Article 25 controls in the DPIA and Article 30 record
- Review all Article 25 controls with DPO quarterly during election periods
- Conduct independent Privacy by Design audit before operational deployment

CHAPTER 8

Privacy Risk Taxonomy and Risk Register

8.1 Risk Scoring Methodology

Privacy risks are assessed using a 5x5 likelihood-impact matrix consistent with ISO/IEC 27005 risk management principles and ENISA's risk assessment framework for large-scale processing operations. Likelihood scores (1-5) represent: 1 = Rare (<5% probability per deployment cycle); 2 = Unlikely (5-20%); 3 = Possible (20-50%); 4 = Likely (50-80%); 5 = Almost Certain (>80%). Impact scores (1-5) represent: 1 = Negligible (no significant effect on data subjects); 2 = Minor (minor inconvenience); 3 = Moderate (significant inconvenience, temporary harm); 4 = Major (significant harm, discriminatory treatment); 5 = Maximum (severe harm, irreversible, affects fundamental rights). Risk score = Likelihood x Impact. Severity bands: 1-4 = LOW; 5-9 = MEDIUM; 10-15 = HIGH; 16-25 = CRITICAL.

Version 2.0 updates: Following the critical review, three risk scores have been elevated: PR-13 (Discrimination/Minority) to CRITICAL (Score 20, from MEDIUM 12); PR-05 (Chilling Effect) to HIGH (Score 15, from MEDIUM 12); and PR-14 (Vulnerable Groups) to HIGH (Score 15, from MEDIUM 10). Three new risk categories have been identified: PR-NEW-01 (Automation Bias), PR-NEW-02 (FIMI Classification Capture), and PR-NEW-03 (Adversarial Evasion).

8.2 Privacy Risk Taxonomy (PR-01 to PR-15 + PR-NEW-01 to PR-NEW-03)

ID	Risk Category	Domain	L	I	Score	Severity
PR-01	Identification/Re-identification Risk: Pseudonymous accounts re-identified through combined analysis of profile, behavioural, and network features	Technical	3	4	12	HIGH
PR-02	Legal Basis Gap: No confirmed Art.6 legal basis for operational political content monitoring; stop-ship condition	Legal	5	5	25	CRITICAL
PR-03	Special Category Data (Political Opinions): NLP pipeline processes Art.9(1) data without confirmed Art.9(2) basis; stop-ship condition	Legal	4	5	20	CRITICAL
PR-04	Transparency Deficit: No Art.14 notice to monitored social media users; systemic transparency failure	Compliance	5	4	20	CRITICAL
PR-05	Chilling Effect on Political Expression: Awareness of FIMI monitoring causes self-censorship and reduces political participation (Penney 2016; Stoycheff 2016) [ELEVATED v2.0]	Societal	3	5	15	HIGH
PR-06	False Positive - Wrongful FIMI Classification: Legitimate political actor classified as FIMI agent; reputational and electoral harm	Technical/AI	4	4	16	CRITICAL
PR-07	Profiling Without Safeguards: Art.22 automated decision-making without explicit safeguards; SCHUFA-compliant human review absent	Legal	4	4	16	CRITICAL

PR-08	Data Breach Risk: Sensitive election-period FIMI data exposed to unauthorised access or exfiltration	Security	3	5	15	HIGH
PR-09	Purpose Creep: Data collected for FIMI monitoring used for other security, commercial, or intelligence purposes	Governance	3	4	12	HIGH
PR-10	Cross-Border Transfer Risk: Personal data transferred to non-EEA countries without adequate safeguards post-Schrems II	Legal	3	4	12	HIGH
PR-11	Data Subject Rights Denial: Failure to respond to SAR, erasure, or objection requests from FIMI-classified accounts	Compliance	3	4	12	HIGH
PR-12	Model Drift and Accuracy Degradation: ML models drift from training distribution over time; false positive rate increases undetected	Technical/AI	4	3	12	HIGH
PR-13	Discrimination/Minority Risk: Russian-speaking minority disproportionately misclassified due to NLP model underperformance on Russian-language content combined with heightened FIMI suspicion in Lithuanian security context; ECHR Art.14, Charter Art.21 [ELEVATED TO CRITICAL v2.0]	Societal	4	5	20	CRITICAL
PR-14	Vulnerable Group Risk: Journalists, activists, civil society actors disproportionately present in politically active monitored population [ELEVATED TO HIGH v2.0]	Societal	3	5	15	HIGH
PR-15	Legislative Basis Inadequacy: Processing relies on general public interest basis without specific FIMI mandate; Art.6(1)(e) gap	Legal	4	4	16	CRITICAL

8.3 New Risk Categories (v2.0)

The following three risk categories were identified during the critical review process and are new in version 2.0:

8.3.1 PR-NEW-01: Automation Bias Risk

Domain: Technical/AI | Likelihood: 3 | Impact: 4 | Score: 12 | Severity: HIGH

Description: Human reviewers systematically confirm AI recommendations due to automation bias (Goddard et al., 2012; Cummings, 2014), effectively converting the human review gate into rubber-stamp approval. Under time pressure during election periods, analysts defer to the automated risk score rather than conducting genuine independent review, engaging Article 22(3) GDPR's requirement for genuine human intervention.

GDPR Provisions: Arts 22(3) (genuine human intervention requirement), 5(1)(d) (accuracy).

Mitigation: (a) Mandatory blind review of 10% random sample of REJECTED alerts each quarter to measure confirmation rate - if confirmation rate for HIGH alerts exceeds 85%, review process must be redesigned; (b) analyst training on automation bias; (c) structured review interface requiring affirmative engagement with specific model features before disposition; (d) monitoring of per-analyst CONFIRM rates.

8.3.2 PR-NEW-02: FIMI Classification Capture Risk

Domain: Governance | Likelihood: 2 | Impact: 5 | Score: 10 | Severity: HIGH

Description: The operational definition of "FIMI" used to train models and configure alert thresholds may be politically captured - used to classify legitimate political opposition or minority political discourse as foreign manipulation. This risk is structural and cannot be fully mitigated by technical controls alone. It affects political opposition actors, minority communities, civil society organisations, and journalists.

GDPR Provisions: Arts 5(1)(a) (fairness), 5(1)(b) (purpose limitation), 9(1) (political opinions); EU Charter Art.21 (non-discrimination), Art.39 (electoral rights).

Mitigation: (a) Civil society and independent academic representation on oversight body; (b) documented and publicly available FIMI classification criteria; (c) annual review of classification criteria with civil society consultation; (d) prohibition on retroactive reclassification of content as FIMI based on political outcome.

8.3.3 PR-NEW-03: Adversarial Evasion Risk

Domain: Technical/AI | Likelihood: 4 | Impact: 3 | Score: 12 | Severity: MEDIUM

Description: Sophisticated FIMI actors adapt tactics to evade detection once aware of the platform's existence, requiring continuous model updating. Each retraining cycle requires collection of new labelled personal data, creating a continuous personal data processing demand not covered by the original DPIA scope. This creates ongoing purpose limitation and storage limitation compliance challenges.

GDPR Provisions: Arts 5(1)(b) (purpose limitation), 5(1)(e) (storage limitation), 35(11) (DPIA review trigger).

Mitigation: Document each model retraining cycle as a DPIA change trigger requiring DPO review. Where retraining requires collection of significantly different data categories, a DPIA update is required. ENISA adversarial robustness testing before each model version deployment.

8.4 Critical and High Risk Mitigation Analysis

8.4.1 PR-13 - Discrimination/Minority Risk [CRITICAL, Score 20]

PR-13 has been elevated to CRITICAL (from MEDIUM in v1.0) following critical review. The Russian-speaking minority in Lithuania (approximately 5-6% of the population) faces compounding discrimination risk: (a) NLP models trained predominantly on Lithuanian-language data systematically underperform on Russian-language content, producing higher false positive rates; (b) Russian-language political content is subject to heightened FIMI suspicion in the Lithuanian security context; (c) wrongful FIMI classification during elections directly affects political participation rights of a national minority under ECHR Art.14 and Charter Art.21. This constitutes a Maximum-severity impact. VDAI consultation under Art.36 is mandatory regardless of other residual risk decisions.

CRITICAL COMPLIANCE GAP: PR-13 CRITICAL: Russian-language model performance failure constitutes a structural discrimination risk against a national linguistic minority. Mandatory Russian-language model validation before deployment and annual subgroup performance reporting are required. VDAI consultation must specifically address PR-13 mitigation.

8.4.2 PR-03 - Article 9 Political Opinion Processing Mitigation

Two mitigation options are available for the Article 9 legal basis gap:

Option A (Preferred): Enact dedicated Lithuanian FIMI monitoring legislation providing a specific Article 9(2)(g) basis. This is the only long-term compliant solution and is the MANDATORY recommendation under REC-L01.

Option B (Interim only): Implement the political opinion feature gate (PBD-D07) to disable explicit political opinion classification outputs pending legislative basis. This may reduce Article 9 exposure during the R&D phase but does not eliminate it.

CRITICAL COMPLIANCE GAP: IMPORTANT LIMITATION (PR-03, Option B): Technical mitigation through the political opinion feature gate reduces but does not eliminate Article 9 exposure. The gate addresses explicit political opinion classification outputs but not the implicit processing of political content patterns within the model inference pipeline. Option B therefore remains an interim partial mitigation, not a substitute for the legislative basis required under Option A. A confirmed Article 9(2) legal basis is required regardless of whether this gate is implemented.

CHAPTER 9

Data Protection Impact Assessment (DPIA)

9.1 DPIA Screening - Mandatory Assessment Confirmed

Article 35(1) GDPR requires a DPIA where processing is likely to result in a high risk to the rights and freedoms of natural persons. Article 35(3) provides three specific categories requiring mandatory DPIA: systematic and extensive evaluation of personal aspects by automated processing (Art.35(3)(a)); processing on a large scale of special category data (Art.35(3)(b)); and large-scale systematic monitoring of publicly accessible areas (Art.35(3)(c)). AICP-FIMI triggers all three specific categories.

EDPB Criterion (WP248 rev.01)	Assessment	AICP-FIMI Finding
1. Evaluation or scoring	YES	Risk scoring (bot probability, FIMI risk score) constitutes systematic evaluation of individuals
2. Automated decision-making with significant effects	YES	FIMI classification may lead to alert transmission to law enforcement - legally significant effect
3. Systematic monitoring	YES	Continuous election-period monitoring of social media users
4. Sensitive data or data of a highly personal nature	YES	Political opinions (Art.9); network associations; political content
5. Data processed on a large scale	YES	Election-period monitoring at national scale involves large numbers of accounts
6. Matching or combining datasets	YES	Network, content, behavioural, and account data combined
7. Data concerning vulnerable data subjects	YES	Includes journalists, activists, political actors, minority communities
8. Innovative use or applying new technological solutions	YES	AI-driven FIMI detection using NLP and network ML is novel technology
9. Processing that prevents data subjects from exercising rights	YES	Covert monitoring prevents effective exercise of transparency/objection rights

KEY FINDING: DPIA MANDATORY: All nine EDPB high-risk criteria are triggered. A formal DPIA is required under Article 35 GDPR before operational deployment. VDAI prior consultation under Article 36 is required given the confirmed high residual risk. The DPIA must be documented, reviewed by the DPO, and submitted to the VDAI with the Article 36 consultation.

9.2 Processing Description

The DPIA covers the following processing operations: (1) Collection of public social media data (account identifiers, content, metadata, network relationships) via API and web collection; (2) NLP-based text analysis generating sentiment, emotionality, linguistic, and political content features; (3) Network analysis generating network graph features and coordination indices; (4) ML model-based risk score assignment (bot probability, FIMI risk score); (5) Human review and alert generation for accounts exceeding risk threshold; (6) Alert and report transmission to clients and potentially law enforcement authorities; (7) Data retention during and after the monitoring period; and (8) Model retraining using accumulated labelled data.

Data subjects affected: All social media users (primarily Lithuanian residents) whose accounts are within the monitoring scope. This includes ordinary citizens, journalists, political activists, politicians, civil society organisations, and Russian-speaking minority members. Data scale: estimated tens of thousands to hundreds of thousands of accounts per election monitoring cycle.

9.3 Necessity and Proportionality Assessment

Article 35(7)(b) requires the DPIA to assess the necessity and proportionality of the processing operations. The necessity test requires that the processing is the least intrusive means of achieving the legitimate aim. The proportionality test requires that the processing does not go beyond what is necessary.

Necessity: The detection of coordinated FIMI campaigns at election scale cannot currently be achieved without automated analysis of large volumes of social media data. Manual monitoring at election scale is not feasible. AI-driven analysis is therefore necessary in principle. However, necessity at the design level must be assessed for each processing operation: collection scope, retention period, and feature extraction must individually satisfy the necessity test.

Proportionality: The proportionality assessment is more challenging. Monitoring of all accounts in a political network - including accounts with no FIMI indicators - to identify the subset that may be engaged in coordination raises proportionality concerns. The ECHR Article 8 surveillance jurisprudence requires that mass monitoring operations have adequate legal basis, limitations, and oversight to be considered proportionate in a democratic society. These requirements are not currently met.

9.4 DPIA Risk Assessment

Risk Scenario	Likelihood	Impact	Risk Level	Proposed Safeguard
Political opinion data processed without Art.9(2) basis (PR-03)	Likely (4)	Maximum (5)	CRITICAL	Legislative basis (REC-L01) or halt NLP political content analysis
Account wrongly classified as FIMI actor; alert transmitted to law enforcement (PR-06)	Likely (4)	Maximum (5)	CRITICAL	Human review gate; accuracy requirement; right to challenge mechanism
Russian-speaking minority accounts disproportionately misclassified (PR-13)	Likely (4)	Maximum (5)	CRITICAL	Russian-language model validation; subgroup fairness audit; VDAI consultation
FIMI classification data shared with law enforcement without LED legal basis (CG-21)	Possible (3)	Maximum (5)	CRITICAL	LED applicability assessment before any alert transmission to law enforcement
No Art.14 transparency notice; data subjects unaware of profiling (PR-04)	Almost Certain (5)	Major (4)	CRITICAL	Art.14 privacy notice published before any data collection commences
Automation bias renders human review nominal; Art.22 safeguards defeated (PR-NEW-01)	Possible (3)	Major (4)	HIGH	Structured review interface; blind audit programme; analyst monitoring
Chilling effect on political discourse measurable at election scale (PR-05)	Possible (3)	Maximum (5)	HIGH	Transparency measures; narrow election-period scope; civil society engagement
Model drift increases false positive rate undetected post-deployment (PR-12)	Likely (4)	Moderate (3)	HIGH	Continuous model monitoring; quarterly performance review; DPO notification trigger

9.5 Safeguards Matrix and Residual Risk

The following safeguards are required to bring risks to an acceptable level:

Safeguard	Addresses	Type	Residual Risk After Safeguard
Legislative mandate (Art.6(1)(e) + Art.9(2)(g))	PR-02, PR-03, PR-15	Legal	LOW if enacted; CRITICAL if not
Art.14 privacy notice publication	PR-04	Organisational	LOW
Russian-language model validation before deployment	PR-13	Technical	HIGH (structural NLP limitation persists)
Subgroup fairness audit (Phase 1, pre-deployment)	PR-13, PR-06	Technical	HIGH - mandatory VDAI consultation required
Genuine human review gate with automation bias safeguards	PR-07, PR-NEW-01	Technical/Organisational	MEDIUM
Art.26 joint controller arrangement with law enforcement	CG-21, PR-02	Legal	LOW if arrangement in place
LED applicability assessment	CG-21	Legal	LOW if assessment completed
Art.10 GDPR legal opinion	CG-22	Legal	LOW if legal opinion confirms no Art.10 data
Political opinion feature gate (PBD-D07)	PR-03	Technical	HIGH - does not replace Art.9(2) basis
Data minimisation controls	PR-01, PR-09	Technical	MEDIUM
End-to-end encryption	PR-08	Technical	LOW
FIMI definition governance with civil society oversight	PR-NEW-02	Governance	MEDIUM
Model retraining DPIA trigger protocol	PR-NEW-03	Organisational	MEDIUM
Blind review audit programme (10% quarterly)	PR-NEW-01	Organisational	MEDIUM
Annual subgroup performance reporting	PR-13	Organisational	HIGH (structural limitation)

CRITICAL COMPLIANCE GAP: RESIDUAL HIGH RISKS AFTER SAFEGUARDS: Even after all proposed safeguards are implemented, PR-13 (Discrimination/Minority) and PR-03 (Political Opinion Processing) retain HIGH residual risk. This level of residual risk makes VDAI prior consultation under Article 36 mandatory and non-optional. The VDAI must be consulted before any operational deployment.

9.6 Prior Consultation - Article 36 GDPR

Article 36(1) GDPR requires the controller to consult the supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. The AICP-FIMI DPIA confirms multiple high and critical residual risks. VDAI prior consultation is mandatory.

Article 36(2) requires that the consultation request include: the respective responsibilities of the controller and processors; the purposes and means of the intended processing; the measures and safeguards provided to protect the rights of data subjects; contact details of the DPO; the DPIA; and any other information requested by the supervisory authority.

9.6.1 Scenario Analysis: VDAI Article 36 Opinion Outcomes [NEW v2.0]

The consortium should not assume that VDAI Article 36 consultation is a formality. For a novel FIMI monitoring system with confirmed residual high risks including political opinion data processing, VDAI scrutiny is likely to be rigorous. Four consultation outcome scenarios are projected:

Scenario A - VDAI approves without conditions: Processing may commence. Document VDAI opinion in the Article 30 record. DPIA review cycle commences. This is the optimal outcome but should not be assumed given the confirmed high residual risks.

Scenario B - VDAI approves subject to conditions: Common conditions may include: time-limitation to specific election periods only; mandatory quarterly reporting to VDAI; independent auditor appointment within defined timeframe; prohibition on specific data categories (e.g., explicit political opinion features). All conditions must be documented, implemented before deployment, and monitored for ongoing compliance. Conditions become legally binding under Article 58(2) GDPR and their breach constitutes a GDPR violation.

Scenario C - VDAI requires suspension pending redesign: Where the VDAI determines that residual risks cannot be adequately mitigated by the proposed safeguards, it may require suspension of deployment pending specific technical or organisational redesign (Article 58(2)(f) GDPR). The consortium must have a project response plan: (a) identify which design change is required; (b) estimate redesign timeline; (c) confirm whether the redesign requires a new DPIA iteration; (d) define the governance process for resuming Article 36 consultation after redesign. The minimum response timeline for Scenario C should be estimated at 3-6 months.

Scenario D - VDAI prohibits processing: Under Article 58(2)(f) GDPR, the VDAI may impose a temporary or permanent ban on processing. A permanent prohibition would render the AICP-FIMI operational model legally unviable in Lithuania without fundamental redesign or new legislative basis. The consortium should assess the probability of this scenario and the commercial and legal implications. Where the probability of Scenario D is assessed as material, the consortium should consider seeking informal pre-consultation with the VDAI before submitting the formal Article 36 DPIA - to identify and resolve the most significant concerns before the formal consultation clock starts.

KEY FINDING: Budget 3-6 months for the VDAI consultation process and allocate DPO and legal counsel time accordingly. Proactive informal engagement with the VDAI before formal submission (as recommended under REC-L07) will reduce the risk of Scenarios C and D.

9.7 DPIA Review Cycle

Article 35(11) GDPR requires the controller to carry out a review of the DPIA where there is a change in the risk represented by processing operations. For AICP-FIMI, mandatory DPIA review triggers include: (1) change in platform scope or functionality (new data sources, new processing operations, new recipient categories); (2) model retraining using significantly different data categories; (3) change in the legal framework (new Lithuanian law; new EDPB guidance; new CJEU judgment affecting the analysis); (4) significant security incident; (5) evidence of systematic misclassification of a data subject group; and (6) annual review as standard practice during deployment.

CHAPTER 10

Ethics and Socio-Technical Alignment

10.1 Democratic Legitimacy and Proportionality

The AICP-FIMI platform operates at the intersection of democratic security (protecting elections from foreign manipulation) and democratic liberty (protecting political expression and participation from surveillance). This tension is fundamental and cannot be resolved by technical design alone - it requires a carefully structured governance framework that maintains democratic accountability over the monitoring system itself.

The ECHR Article 8 framework for surveillance systems in democratic societies requires: (a) a legal basis of sufficient quality (accessible, foreseeable, and adequate safeguards); (b) a legitimate aim; (c) necessity in a democratic society; and (d) proportionality. The ECtHR's "Big Brother Watch and Others v UK" (App. 58170/13) confirms that bulk interception of communications requires robust oversight, end-to-end safeguards, and cannot be justified by mere security interests alone. These principles apply by analogy to large-scale social media monitoring during elections.

10.2 Human Oversight and Accountability Framework

Genuine human oversight - as opposed to nominal human review - is essential for the ethical and legally compliant operation of AICP-FIMI. Human oversight requirements at four levels:

Operational level: Individual alert review by trained analysts with structured interface requiring engagement with model features. Automation bias safeguards as specified in Section 7.2.6. Genuine override authority.

Management level: DPO oversight of processing operations, access logs, and alert disposition patterns. Quarterly reporting to senior management. Escalation protocol for systematic issues.

Independent oversight level: External independent auditor with access to model performance data, subgroup fairness metrics, and alert disposition statistics. Annual published report. Civil society representation on oversight board.

Regulatory level: VDAI prior consultation and ongoing notification. Article 36 consultation before deployment. Annual report to VDAI during deployment.

10.3 Transparency and Explainability

Transparency Dimension	Requirement	Implementation
Public transparency about system existence	Data subjects must know that FIMI monitoring exists (Art.14 GDPR)	Publish Art.14 privacy notice on AICP-FIMI project website and VDAI register
Transparency about FIMI classification criteria	Fairness requires that classification criteria are publicly documented	Publish summary FIMI classification framework (without disclosing operational details that would enable gaming)
Explainability of individual classifications	Individuals subject to FIMI classification entitled	Implement XAI module providing natural-language explanation of top model features

	to explanation under Art.22(3)	
Transparency to oversight body	Independent oversight requires access to model architecture, training data, and performance statistics	Grant oversight auditor access to model documentation and performance logs
Transparency to VDAI	Art.36 consultation requires complete transparency about processing	Submit complete DPIA including all risk registers and safeguards

10.4 Fairness and Non-Discrimination

The obligation of fairness under Article 5(1)(a) GDPR and the non-discrimination principle under EU Charter Article 21 require that the AICP-FIMI system does not produce systematically different outcomes for different social groups. Subgroup fairness analysis is required across: (a) language groups (Lithuanian vs. Russian vs. English content); (b) political orientation (left, right, centrist, minority political views); (c) account type (individual vs. organisation vs. media); and (d) geographic origin (Lithuanian accounts vs. foreign accounts posting in Lithuanian).

Fairness thresholds must be defined before deployment. Minimum requirement: precision and recall must not differ by more than 10 percentage points across language groups. The Russian-language subgroup must meet the same minimum precision threshold as the Lithuanian-language subgroup. Any systematic performance gap above this threshold is a deployment-blocking issue pending remediation.

10.5 Stakeholder and Affected Group Analysis

Group	FIMI Risk Exposure	Privacy Risk	Safeguard Required
General social media users	Low - most not flagged	Medium - data collected without notice	Art.14 notice; data minimisation; retention limits
Politically active users	Medium - in monitoring scope	High - political content analysed	Art.9 legal basis; feature gate; right to object
Journalists and media	High - high political activity, FIMI suspicion proximity	Very High - false positive risk, chilling effect	Vulnerable group flag; mandatory human review for media accounts
Opposition politicians	High - political opposition may be miscategorised	Very High - false positive affects electoral rights	FIMI definition governance; civil society oversight
Russian-speaking minority	High - structural NLP disadvantage	Critical - compounding discrimination risk (PR-13)	Russian-language model validation; subgroup audit; VDAI consultation required
Civil society organisations	Medium-High - politically active	High - potential misclassification	FIMI classification capture safeguards (PR-NEW-02)
Foreign state agents (intended targets)	High - intended targets of system	Low (privacy interests subordinate to legitimate monitoring)	Proportionate response; legal basis required

10.6 Misuse and Overreach Safeguards

The most serious societal risk from AICP-FIMI is not technical failure but political misuse - deployment of the system to suppress legitimate political opposition or minority political expression under the cover of FIMI detection. Structural safeguards required:

- Independent oversight board with civil society and academic representation, not exclusively government or security sector
- Publicly documented FIMI classification criteria reviewed annually with civil society consultation
- Prohibition on using AICP-FIMI outputs as the sole basis for any adverse action against individuals or organisations
- Mandatory judicial authorisation before any AICP-FIMI alert is used in criminal proceedings
- Sunset clause - AICP-FIMI operational authorisation expires after each election cycle and requires renewal with fresh DPIA
- Independent annual audit of classification outcomes with statistical analysis of subgroup outcomes
- Whistleblower protection for AICP-FIMI personnel who report misuse or overreach to the VDAI
- Parliamentary oversight committee with access to aggregated operational statistics

CHAPTER 11

Standards and Best Practices

11.1 ISO/IEC Standards Applicability

Standard	Title	Applicability to AICP-FIMI	Key Requirements
ISO/IEC 27001:2022	Information security management systems	Recommended certification for Acrux as cloud platform operator	ISMS implementation; risk management; security controls; audit
ISO/IEC 27701:2019	Privacy Information Management System (PIMS)	Highly recommended - GDPR compliance certification pathway	PIMS controls; data subject rights; PbD; vendor management
ISO/IEC 27005:2022	Information security risk management	Methodology for privacy risk register and DPIA risk assessment	Risk taxonomy; likelihood/impact assessment; risk treatment
ISO/IEC 23894:2023	AI risk management	Applicable to ML model risk management in AICP-FIMI	AI risk taxonomy; model lifecycle risk; human oversight
ISO/IEC 42001:2023	AI management systems	Framework for AI governance of AICP-FIMI platform	AI impact assessment; governance; transparency; accountability

11.2 NIST Frameworks

NIST Privacy Framework (2020): Provides a voluntary framework for improving privacy through enterprise risk management. The five functions - Identify, Govern, Control, Communicate, Protect - align directly with the AICP-FIMI compliance requirements. Adoption of the NIST Privacy Framework is recommended as a supplementary governance tool alongside ISO/IEC 27701.

NIST AI Risk Management Framework (AI RMF 1.0, 2023): Provides structured AI risk management guidance through four core functions: Govern (organisational AI risk governance); Map (context and risk identification); Measure (analysis and assessment); Manage (risk treatment and monitoring). The AI RMF aligns closely with AI Act conformity assessment requirements and is recommended for VilniusTech and KTU model development governance.

11.3 ENISA Guidance

ENISA Guidelines on Security Measures under Article 32 GDPR provide a structured approach to implementing technical and organisational measures proportionate to the risks. For AICP-FIMI, ENISA guidance on: (a) personal data pseudonymisation; (b) cloud security; (c) AI security (ENISA AI Security Guidelines 2023); and (d) cybersecurity for electoral infrastructure is particularly relevant.

11.4 EDPB Guidelines Compliance Matrix

EDPB Guideline	Topic	Application to AICP-FIMI

WP248 rev.01 (EDPB endorsed)	DPIA - 9 criteria	Mandatory DPIA screening methodology - all 9 criteria triggered
Guidelines 4/2019	Art.25 Privacy by Design and Default	Eight data protection goals operationalised in Chapter 7
Guidelines 1/2024	Legitimate Interest	LI three-part test applied in Section 5.2.2
Guidelines 8/2020	Targeting social media users	Confirms social media monitoring constitutes personal data processing
Guidelines 5/2020	Consent	Confirms consent unavailable for covert monitoring
Guidelines 01/2022	Art.25 implementation	Privacy by Default settings matrix (Chapter 7)
Recommendations 01/2020	Supplementary transfer tools (Schrems II)	Transfer impact assessment requirement for cloud providers

CHAPTER 12

Case Law and Supervisory Guidance

12.1 Key CJEU Judgments

12.1.1 SCHUFA - C-634/21 (2023): Automated Decision-Making

CJEU (Grand Chamber), C-634/21, ECLI:EU:C:2023:957. The Court held that an automated creditworthiness probability score constitutes an "automated decision" within the meaning of Article 22(1) GDPR where the score "determines in a decisive manner" the human decision that follows. This significantly expands the scope of Article 22 - a nominal human review step does not escape Article 22 if the human systematically follows the automated score. Applied to AICP-FIMI: where automation bias causes analysts to routinely confirm automated risk scores, the Article 22 safeguards apply. Relevant safeguards under Art.22(2): legal authorisation or explicit consent; and under Art.22(3): meaningful information, right to human review, right to contest.

12.1.2 Latvijas Padomju - C-439/19 (2021): Political Data and Public Accessibility

CJEU, C-439/19, ECLI:EU:C:2021:504. The Court held that systematic online publication of data about individuals' political activities (in this case, as members of the former Soviet Communist Party) constitutes processing of special category data under Article 9(1) GDPR, even where the data was previously publicly accessible. The judgment directly refutes the argument that public social media data cannot constitute special category data. It confirms that systematic automated processing of political content for FIMI detection purposes engages Article 9(1) regardless of the public accessibility of the source data.

12.1.3 Meta Platforms Ireland v Bundeskartellamt - C-252/21 (2023): Sensitive Data Processing

CJEU, C-252/21, ECLI:EU:C:2023:537. The Court held that special category data under Article 9 GDPR can be processed for the purposes of personalised advertising only under the exhaustive exceptions of Article 9(2), and confirmed that data which "reveals" special characteristics (including political opinions) through combination and analysis engages Article 9 protection even if the source data is not inherently special category. This is directly applicable to AICP-FIMI: NLP analysis that generates inferences about political orientation from ordinary text content engages Article 9(1) because the output "reveals" political opinions within the meaning of the judgment. NOTE v2.0 correction: The referring court was the Bundesgerichtshof (German Federal Court of Justice); the DPA involved was the Bundeskartellamt (German Federal Cartel Office). This case did not involve the HDPA (Hellenic Data Protection Authority).

12.1.4 Schrems II - C-311/18 (2020): International Data Transfers

CJEU (Grand Chamber), C-311/18, ECLI:EU:C:2020:559. Invalidated the Privacy Shield adequacy decision and imposed Transfer Impact Assessment requirements for SCCs. Directly applicable to AICP-FIMI cloud infrastructure transfers to the US.

12.1.5 Digital Rights Ireland - Joined Cases C-293/12 and C-594/12 (2014)

CJEU (Grand Chamber). The Court established that even temporary mass retention of communications data constitutes a serious interference with fundamental rights. The proportionality analysis from Digital

Rights Ireland - requiring strict necessity, clear limitation, robust oversight - applies to AICP-FIMI's election-period monitoring scope.

12.1.6 Satamedia - C-73/07 (2008): Public Data and GDPR Applicability

CJEU, C-73/07, ECLI:EU:C:2008:727. The Court confirmed that systematic collection and dissemination of publicly available personal data (in that case, tax information) constitutes processing of personal data subject to full data protection law obligations. Supports the analysis in Section 4.1 that public social media data collection is fully subject to GDPR.

12.2 Key ECtHR Judgments

12.2.1 Big Brother Watch v UK - App. 58170/13 (2021)

ECtHR (Grand Chamber). The Court held that bulk interception of communications for national security purposes can be compatible with Article 8 ECHR only where: the legal basis is accessible and foreseeable; the system includes adequate safeguards; there is independent oversight; and individuals have access to effective remedies. These requirements apply by analogy to AICP-FIMI election-period bulk monitoring.

12.2.2 Benedik v Slovenia - App. 62357/14 (2018)

ECtHR. Confirmed that online pseudonymous identifiers (IP addresses) constitute private information within the scope of Article 8 ECHR. Online monitoring must comply with the Article 8 lawfulness, necessity, and proportionality requirements.

12.3 VDAI and DPA Guidance

The VDAI (Valstybine duomenu apsaugos inspekcija) is the competent supervisory authority for AICP-FIMI processing in Lithuania. VDAI guidance on DPIA, legitimate interest assessment, and high-risk processing should be consulted alongside EDPB guidelines. The VDAI's prior consultation process under Article 36 GDPR is the primary regulatory interaction point for the consortium before deployment. The VDAI has published guidance on DPIA methodology and the list of processing operations requiring mandatory DPIA under Lithuanian law.

12.4 AI Act Compliance Analysis

The EU AI Act (Regulation 2024/1689) creates a risk-based regulatory framework for AI systems. AICP-FIMI likely qualifies as a high-risk AI system under Annex III, triggering conformity assessment, CE marking, technical documentation, post-market monitoring, and registration requirements. The AI Act also establishes a Fundamental Rights Impact Assessment (FRIA) requirement for deploying entities under Article 27, which is distinct from the DPIA and should be conducted in addition to it.

12.4.1 AI Act Article 5 - Prohibited AI Practices: Assessment [NEW v2.0]

Article 5 AI Act establishes a list of prohibited AI practices. Three Article 5 prohibitions are assessed for AICP-FIMI:

Art.5(1)(c) - Social Scoring Prohibition: Article 5(1)(c) prohibits AI systems used by public authorities to evaluate or classify natural persons based on their social behaviour or personal characteristics, leading to detrimental treatment in unrelated social contexts. Assessment: AICP-FIMI is not used by a public authority (it is a private system); its outputs are limited to FIMI classification rather than general social scoring; and consequences are limited to the election integrity context, not unrelated social contexts. AICP-FIMI does not meet the Art.5(1)(c) prohibition criteria on current design. ASSUMPTION: If the platform is procured and

operated directly by a public authority, this assessment must be revisited - state-operated AICP-FIMI may engage Art.5(1)(c).

Art.5(1)(h) - Real-Time Remote Biometric Identification: Article 5(1)(h) prohibits real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes. Assessment: AICP-FIMI analyses social media accounts (not physical spaces) and does not use biometric identification. This prohibition does not apply on current design.

Art.5(1)(b) - Subliminal Techniques: Article 5(1)(b) prohibits AI systems that deploy subliminal techniques to distort behaviour in ways that cause harm. AICP-FIMI is a detection tool, not a behavioural manipulation system. This prohibition does not apply.

KEY FINDING: AI Act Article 5 Assessment: AICP-FIMI does not engage any Article 5 prohibition on its current design as a private-sector detection tool. However, the Article 5 assessment should be reviewed if the platform's scope is expanded to include: facial recognition of profile images; physical location tracking; state procurement and operation as a public authority tool; or use by law enforcement as a primary investigative tool.

12.5 Orange Romania - C-61/19 (2020): Consent and LI Necessity

CJEU, C-61/19, ECLI:EU:C:2020:901. The Court confirmed that the necessity element of the legitimate interest basis must be rigorously assessed - the fact that processing is useful or convenient does not make it necessary. This supports the analysis in Section 5.2.2 that the LI three-part test is stringent and cannot be assumed satisfied for large-scale political content monitoring.

12.6 ASNEF - Joined Cases C-468/10 and C-469/10 (2011)

CJEU, Joined Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777. The Court confirmed that the legitimate interest basis requires a balanced assessment giving appropriate weight to both the controller's interest and the data subjects' expectations and rights. The fact that data subjects had not objected does not substitute for a genuine balancing exercise.

CHAPTER 13

Compliance Gap Register

13.1 Gap Register Overview

The compliance gap register identifies all GDPR and related regulatory compliance gaps identified in the AICP-FIMI analysis. Version 2.0 contains 22 compliance gaps: 7 CRITICAL, 10 HIGH, and 5 MEDIUM. Two new CRITICAL gaps (CG-21 and CG-22) were identified in the critical review process. Each gap entry includes the parent risk category (PR-xx) for cross-referencing with the risk register in Chapter 8.

13.2 Critical Compliance Gaps (CG-01 to CG-07)

Gap ID	Severity	Description	GDPR Article	Parent Risk	Required Action	Deadline
CG-01	CRITICAL	No Art.6(1)(e) legislative basis for FIMI monitoring at election scale	Art.6(1)(e)	PR-02, PR-15	Engage Lithuanian Parliament for dedicated FIMI monitoring legislation	Before deployment
CG-02	CRITICAL	No Art.9(2) basis for processing political opinion data inferred by NLP	Art.9(1)/(2)	PR-03	Legislative basis required (Art.9(2)(g)) or halt political content NLP	Before deployment
CG-03	CRITICAL	No Art.14 transparency/privacy notice published for monitored users	Art.14	PR-04	Publish GDPR Art.14 privacy notice on project website before any collection	Before data collection
CG-04	CRITICAL	Art.22 profiling safeguards absent; automated decision-making without genuine human oversight	Art.22	PR-07	Implement SCHUFA-compliant genuine human review; automation bias safeguards	Before operational use
CG-05	CRITICAL	No confirmed Art.6 legal basis for false positive - wrongly classified individuals subject to alert	Art.6; Art.5(1)(a)	PR-06	Accuracy mechanism; right to challenge; human review gate	Before deployment
CG-21	CRITICAL	Law Enforcement Directive intersection not assessed - LED governs law enforcement recipient processing	Art.2 LED; Art.6 GDPR	PR-02	Conduct LED applicability assessment before any law enforcement alert transmission [NEW v2.0]	Before VDAI submission
CG-22	CRITICAL	Art.10 GDPR criminal offences data assessment absent - FIMI classification may constitute offences data	Art.10 GDPR	PR-03	Commission formal legal opinion on Art.10 applicability to FIMI classification data [NEW v2.0]	Before VDAI submission

13.3 High Priority Gaps (CG-06 to CG-15)

Gap ID	Severity	Description	GDPR Article	Parent Risk	Required Action
CG-06	HIGH	Data retention schedule undefined; no Art.5(1)(e) storage limitation policy	Art.5(1)(e)	PR-01	Define retention schedule per data category; technical enforcement
CG-07	HIGH	Article 30 records of processing activities not drafted	Art.30	PR-09	Draft Art.30 records before any data collection; update for each processing change
CG-08	HIGH	Article 28 processor agreements not in place with VilniusTech, KTU, cloud providers	Art.28	PR-01	Execute Art.28 agreements with all processors before data sharing
CG-09	HIGH	Article 26 joint controller arrangements not in place with potential co-controllers	Art.26	PR-02	Execute Art.26 arrangements with law enforcement authorities and clients
CG-10	HIGH	DPO not yet appointed; appointment mandatory under Art.37(1)(b)/(c)	Art.37	PR-04	Appoint DPO before any personal data collection commences
CG-11	HIGH	Data minimisation controls not implemented at collection layer	Art.5(1)(c)	PR-01	Implement field-level minimisation; time-window restriction; threshold-gated collection
CG-12	HIGH	Pseudonymisation not implemented for non-production environments	Art.25; Art.32	PR-08	Implement pseudonymisation pipeline for R&D environments
CG-13	HIGH	Transfer impact assessment (TIA) not conducted for non-EEA cloud infrastructure	Art.44-49	PR-10	Conduct TIA per Schrems II for each non-EEA data transfer; SCC review
CG-14	HIGH	No data subject rights handling procedure; Art.15-22 rights not operationalised	Arts.15-22	PR-11	Implement SAR handling procedure; right to object mechanism; accuracy correction
CG-15	HIGH	No model performance monitoring or drift detection mechanism	Art.5(1)(d); Art.22	PR-12	Implement continuous model monitoring; quarterly performance review; DPO trigger

13.4 Medium Priority Gaps (CG-16 to CG-22 Medium)

Gap ID	Severity	Description	GDPR Article	Parent Risk	Required Action
CG-16	MEDIUM	No security incident response plan aligned to Art.33/34 breach notification	Art.33/34	PR-08	Draft incident response plan; 72h VDAI notification procedure
CG-17	MEDIUM	Subgroup fairness audit not planned for pre-deployment phase	Art.5(1)(a)/(d)	PR-13	Conduct subgroup fairness audit Phase 1 (pre-deployment) per Section 15.2
CG-18	MEDIUM	No FIMI classification criteria governance; risk of political capture	Art.5(1)(a)	PR-NEW-02	Establish FIMI definition governance board with civil society representation

CG-19	MEDIUM	NIS2 qualification assessment not conducted for Acrux as managed security service provider	Art.21 NIS2	PR-08	Acrux legal counsel to assess NIS2 Annex II qualification before deployment
CG-20	MEDIUM	AI Act conformity assessment not commenced for high-risk AI system classification	AI Act Annex III	PR-06	Commence AI Act conformity assessment and FRIA; registration in EU AI database

Gap Register Summary: 22 total compliance gaps - 7 CRITICAL (must resolve before deployment), 10 HIGH (must resolve before deployment or as priority implementation), 5 MEDIUM (resolve before or during Phase 1 deployment). All CRITICAL gaps are deployment-blocking stop-ship conditions.

CHAPTER 14

Recommendations

14.1 Classification Framework

Recommendations are classified in three tiers: MANDATORY - required by law (GDPR, AI Act, LED, or other binding instrument); BEST PRACTICE - strongly recommended as the standard of care expected by a competent DPO and supervisory authority, derived from EDPB guidance, CJEU case law, and ISO/IEC standards; ADVISORY - project-specific recommendation based on the risk profile of AICP-FIMI that goes beyond legal minimum.

14.2 Legal Recommendations (REC-L01 to REC-L09)

ID	Recommendation	Class	Addresses	Timeline
REC-L01	Seek enactment of dedicated Lithuanian FIMI monitoring legislation providing Art.6(1)(e) basis and Art.9(2)(g) basis with appropriate safeguards	MANDATORY	CG-01, CG-02	Before deployment
REC-L02	Commission formal legal opinion on Art.10 GDPR applicability to FIMI classification data	MANDATORY	CG-22	Before VDAI submission
REC-L03	Conduct LED applicability assessment for each intended law enforcement alert recipient	MANDATORY	CG-21	Before any law enforcement transmission
REC-L04	Execute Article 28 processor agreements with VilniusTech, KTU, and all cloud providers	MANDATORY	CG-08	Before data sharing commences
REC-L05	Execute Article 26 joint controller arrangements with law enforcement authorities and client organisations where applicable	MANDATORY	CG-09	Before alert transmission
REC-L06	Appoint Data Protection Officer before any personal data collection commences	MANDATORY	CG-10	Immediately
REC-L07	Engage in informal pre-consultation with VDAI before formal Art.36 submission	BEST PRACTICE	CG-01, CG-02	Phase 0
REC-L08	Publish Article 14 privacy notice before any social media data collection	MANDATORY	CG-03	Before data collection
REC-L09	Conduct Transfer Impact Assessment for all non-EEA cloud infrastructure transfers	MANDATORY	CG-13	Before cloud deployment

14.3 Technical Recommendations (REC-T01 to REC-T12)

ID	Recommendation	Class	Addresses	Timeline
REC-T01	Implement field-level data minimisation at API collection layer with DPO-approved field allowlist	MANDATORY	CG-11	Phase 0
REC-T02	Implement pseudonymisation for all R&D and non-production environments	MANDATORY	CG-12	Phase 0

REC-T03	Deploy role-based access control with least-privilege defaults and quarterly access review	MANDATORY	CG-07	Phase 0
REC-T04	Implement end-to-end encryption (AES-256 at rest; TLS 1.3 in transit) with HSM key management	MANDATORY	CG-16	Phase 0
REC-T05	Deploy comprehensive audit logging with tamper-evident signing for all data access and alert disposition events	MANDATORY	CG-07	Phase 0
REC-T06	Implement genuine human review gate with structured interface requiring engagement with top-5 model features	MANDATORY	CG-04	Phase 1
REC-T07	Implement political opinion feature gate (PBD-D07) with DPO-controlled activation pending Art.9(2) basis confirmation	MANDATORY	CG-02	Phase 1
REC-T08	Deploy continuous model performance monitoring with drift detection and DPO notification trigger	MANDATORY	CG-15	Phase 1
REC-T09	Target minimum 95% precision threshold for FIMI alert system to ensure proportionality at election scale	BEST PRACTICE	CG-05	Phase 1
REC-T10	Conduct subgroup fairness audit before deployment: precision/recall analysis across language groups, political content categories, and account types	MANDATORY	CG-17	Phase 1 pre-deployment
REC-T11	Implement XAI (explainable AI) module for Art.22(3) explanation of individual classifications	BEST PRACTICE	CG-04	Phase 1
REC-T12	Deploy automated retention enforcement with cryptographic erasure and DPO confirmation workflow	MANDATORY	CG-06	Phase 0

NOTE ON REC-T09 CLASSIFICATION (v2.0 correction): REC-T09 is classified as BEST PRACTICE rather than MANDATORY. No GDPR provision, EDPB guideline, or CJEU judgment mandates a specific quantitative accuracy threshold for AI systems. The 95% threshold is derived from the proportionality principle (Art.5(1)(c) data minimisation and Art.5(1)(d) accuracy) and the specific risk profile of AICP-FIMI - where 5% false positives at election scale produces a significant volume of wrongly identified individuals. The threshold represents the minimum standard required for proportionate processing given this risk profile, not a general legal rule. Controllers with different risk profiles may apply different thresholds with corresponding proportionality justification. This classification was MANDATORY in v1.0 and has been corrected.

14.4 Governance Recommendations (REC-G01 to REC-G11)

ID	Recommendation	Class	Addresses	Timeline
REC-G01	Establish independent oversight board with civil society and academic representation for AICP-FIMI operations	BEST PRACTICE	PR-NEW-02	Phase 0
REC-G02	Develop and publish FIMI classification criteria with annual civil society review	BEST PRACTICE	CG-18	Phase 1
REC-G03	Implement quarterly blind review audit of 10% of REJECTED alerts to measure and control automation bias	BEST PRACTICE	PR-NEW-01	Phase 1
REC-G04	Establish DPIA review cycle with mandatory triggers for scope changes and model retraining	MANDATORY	PR-NEW-03	Ongoing

REC-G05	Draft and submit formal Art.36 DPIA to VDAI with DPO sign-off	MANDATORY	All CRITICAL	Before deployment
REC-G06	Implement data subject rights handling procedure (SAR, erasure, objection, rectification)	MANDATORY	CG-14	Phase 0
REC-G07	Draft and implement incident response plan aligned to Art.33/34 and NIS2 Art.23 notification obligations	MANDATORY	CG-16	Phase 0
REC-G08	Conduct AI Act conformity assessment and Fundamental Rights Impact Assessment (FRIA) for high-risk AI system	MANDATORY	CG-20	Phase 1
REC-G09	Implement sunset clause requiring AICP-FIMI operational authorisation renewal after each election cycle with fresh DPIA	ADVISORY	PR-NEW-02	Phase 0 design
REC-G10	Provide mandatory automation bias training for all alert review analysts before deployment	BEST PRACTICE	PR-NEW-01	Phase 1
REC-G11	Conduct annual subgroup fairness performance report with outcome statistics for Russian-language and minority accounts	MANDATORY	PR-13	Annual from deployment

CHAPTER 15

Implementation Roadmap

15.1 Phase 0 - Pre-Deployment Foundation (Months 1-3)

Phase 0 must be completed before any personal data collection commences. All CRITICAL compliance gaps in Phase 0 are absolute prerequisites.

ID	Action	Owner	Reference	Target
P0-01	Appoint Data Protection Officer (DPO)	Acrux CEO	REC-L06; Art.37	Month 1
P0-02	Commence legislative mandate engagement with Lithuanian Parliament	Acrux Legal; MRU	REC-L01; CG-01	Month 1
P0-03	Commission Art.10 GDPR formal legal opinion on FIMI classification data	Acrux Legal	REC-L02; CG-22	Month 1
P0-04	Conduct LED applicability assessment for law enforcement recipients	DPO; Acrux Legal	REC-L03; CG-21	Month 1
P0-05	Publish Art.14 privacy notice on AICP-FIMI website	DPO; Comms	REC-L08; CG-03	Month 2
P0-06	Execute Art.28 processor agreements with VilniusTech, KTU, cloud providers	Acrux Legal; DPO	REC-L04; CG-08	Month 2
P0-07	Execute Art.26 joint controller arrangements where applicable	DPO; Acrux Legal	REC-L05; CG-09	Month 2
P0-08	Draft Art.30 records of processing activities	DPO	CG-07	Month 2
P0-09	Engage VDAI in informal pre-consultation	DPO; Acrux Legal	REC-L07	Month 2-3
P0-10	Implement field-level data minimisation at collection layer	ML Lead; DPO	REC-T01; CG-11	Month 2
P0-11	Implement pseudonymisation for R&D environments	ML Lead; Security	REC-T02; CG-12	Month 2
P0-12	Deploy role-based access control and encryption	Security Lead	REC-T03; REC-T04	Month 2-3
P0-13	Implement audit logging with tamper-evident signing	Security Lead; DPO	REC-T05	Month 3
P0-14	Implement automated retention enforcement and deletion pipeline	Engineering Lead; DPO	REC-T12; CG-06	Month 3
P0-15	Draft incident response plan (Art.33/34; NIS2 Art.23)	DPO; Security Lead	REC-G07; CG-16	Month 3
P0-16	Implement data subject rights handling procedure	DPO; Engineering	REC-G06; CG-14	Month 3

15.2 Phase 1 - Pre-Deployment Validation (Months 4-6)

Phase 1 includes technical deployment preparation and compliance validation. Deployment is conditional on completing all Phase 1 items.

ID	Action	Owner	Reference	Target

P1-01	Implement genuine human review gate with structured feature engagement interface	Engineering; DPO	REC-T06; CG-04	Month 4
P1-02	Implement political opinion feature gate (PBD-D07) with DPO-controlled activation	ML Lead; DPO	REC-T07; CG-02	Month 4
P1-03	Deploy continuous model performance monitoring with drift detection	ML Lead	REC-T08; CG-15	Month 4
P1-04	Deploy XAI module for Art.22(3) individual classification explanations	ML Lead; Engineering	REC-T11	Month 5
P1-05	Establish FIMI classification governance board with civil society representation	Acrux Management; DPO	REC-G01; REC-G02	Month 4
P1-06	Deliver automation bias training for all alert review analysts	DPO; HR	REC-G10; PR-NEW-01	Month 5
P1-07	Commence AI Act conformity assessment and FRIA	DPO; Legal	REC-G08; CG-20	Month 4
P1-08	Assess NIS2 qualification (Acrux as managed security service provider)	Acrux Legal	CG-19	Month 4
P1-09	Confirm Transfer Impact Assessments for all non-EEA infrastructure	DPO; Legal	REC-L09; CG-13	Month 4
P1-10	Draft formal DPIA for VDAI Art.36 submission with DPO sign-off	DPO; MRU; Acrux Legal	REC-G05	Month 5
P1-11	Submit DPIA for VDAI prior consultation under Art.36	DPO; Acrux Legal	REC-G05; CG-01	Month 5-6
P1-12	Prepare and brief VDAI consultation response team	DPO; Acrux Legal; MRU	Section 9.6.1	Month 6
P1-13	Confirm legislative mandate status; proceed only if basis confirmed or interim basis agreed	Acrux Legal; DPO	REC-L01; CG-01	Month 6
P1-14	Conduct Russian-language model validation: precision/recall analysis vs Lithuanian-language baseline	ML Lead; DPO	PR-13; REC-G11	Month 5
P1-15	Conduct pre-deployment subgroup fairness audit: precision/recall/F1 across language, political content, account type subgroups. Deployment conditional on meeting fairness thresholds. | Reference: REC-T10; CG-17	ML Lead; DPO	REC-T10; PR-13	Month 4-5

15.3 Phase 2 - Initial Deployment (Months 7-12)

ID	Action	Owner	Reference	Target
P2-01	Deploy AICP-FIMI in restricted pilot scope following VDAI authorisation	Acrux Product; DPO	All CRITICAL gaps resolved	Month 7
P2-02	Activate human review gate and audit logging in production	Engineering; DPO	REC-T06; REC-T05	Month 7
P2-03	Begin DPO oversight cycle: weekly review during first election monitoring period	DPO	Art.39; Art.30	Ongoing
P2-04	Implement blind review audit (10% quarterly) to measure automation bias	DPO; Senior Analyst	REC-G03; PR-NEW-01	Month 8
P2-05	Conduct first live-data subgroup fairness audit using operational data from first 60 days of deployment. Compare against pre-deployment baseline. Report deviations to DPO and oversight body. Frequency: Quarterly thereafter.	ML Lead; DPO	REC-T10; PR-13	Month 9

P2-06	Begin AI Act registration in EU AI database upon conformity assessment completion	Legal; DPO	AI Act Art.49	Month 10
P2-07	Publish first transparency report on AICP-FIMI operations (anonymised/aggregated)	DPO; Comms	REC-G02; Art.5(2)	Month 12

15.4 Phase 3 - Ongoing Compliance (Annual)

P3-01Annual DPIA review per Art.35(11)DPO; MRUArt.35(11)Annual	P3-02Annual subgroup fairness audit report with Russian-language and minority statisticsML Lead; DPOREC-G11; PR-13Annual	P3-03Annual FIMI classification criteria review with civil society consultationOversight BoardREC-G02; PR-NEW-02Annual	P3-04Model retraining DPIA update assessment (each retraining cycle)DPO; ML LeadPR-NEW-03; Art.35(11)Per cycle	P3-05Annual Art.36 compliance report to VDAIDPO Art.36; Art.58Annual	P3-06AICP-FIMI sunset review - operational authorisation renewal Acrux Management; DPOREC-G09Post-election cycle	P3-07Legislative mandate review - confirm continued adequacy of statutory basisAcrux Legal; MRUCG-01Annual	P3-08AI Act post-market monitoring reportDPO; LegalAI Act Art.72Annual	P3-09Independent privacy audit by external auditorAcrux ManagementBEST PRACTICEAnnual	P3-10Parliamentary oversight committee briefing (aggregated statistics)Acrux Management; DPORECdemocratic safeguards Annual
I	D								
A	c	t	i	o	n				
O	w	n	e	r					
R	e	f	e	r	e	n	c	e	
T	a	r	g	e	t				

CHAPTER 16

Conclusions

16.1 Principal Findings

The AICP-FIMI platform addresses a genuine and pressing public interest need: the protection of democratic elections from foreign information manipulation. The project is technically ambitious and potentially valuable. However, the MRU compliance analysis finds that the platform cannot be lawfully deployed in Lithuania - or elsewhere in the EU - in its current form without resolving a set of fundamental GDPR compliance gaps.

The two principal stop-ship conditions are: first, the absence of a confirmed legal basis under Article 6(1)(e) GDPR for the operational-scale processing of political content social media data - requiring a dedicated Lithuanian legislative mandate; and second, the absence of an Article 9(2) basis for processing data that reveals political opinions through NLP inference - requiring either the same legislative mandate or a halt to the political content NLP features pending enactment.

Two additional stop-ship conditions were identified in the critical review (v2.0 additions): the absence of a Law Enforcement Directive (LED) intersection analysis for alert recipients who are law enforcement authorities; and the absence of an Article 10 GDPR assessment for FIMI classification data where FIMI operations are criminalised under Lithuanian law.

Beyond the stop-ship conditions, 18 further compliance gaps across legal, technical, and governance dimensions require resolution. The full set of 22 compliance gaps, with their severity classifications and required actions, is documented in Chapter 13.

16.2 Path to Compliance

The path to compliant deployment of AICP-FIMI is achievable but requires concerted effort across legal, technical, and governance dimensions. The most critical single action is the legislative mandate - without which no amount of technical privacy engineering will fully resolve the Article 6 and Article 9 gaps. MRU strongly recommends that the consortium engage with Lithuanian legislative authorities from the earliest stage of the project, treating the legislative mandate as a Phase 0 prerequisite rather than a Phase 2 follow-up.

The DPIA and VDAI prior consultation process is the central compliance gate. The consortium should approach the VDAI not as a formality but as a substantive regulatory engagement, budgeting 3-6 months for the consultation process and allocating adequate DPO and legal counsel resources. Proactive informal engagement with the VDAI before formal submission is strongly recommended.

16.3 Version 2.0 Improvements Summary

This version 2.0 report incorporates all corrections and enhancements identified in the formal critical review (AICP-MRU-CRITICAL-REVIEW-RESULTS-v1.0). The principal improvements are: two new critical legal analyses (LED Section 5.9 and Art.10 Section 5.2.3); three elevated risk scores (PR-13 to CRITICAL, PR-05 and PR-14 to HIGH); three new risk categories (PR-NEW-01/02/03); enhanced VDAI consultation scenario analysis (Section 9.6.1); corrected Meta case labelling; reclassified REC-T09; subgroup fairness audit moved to Phase

1; AI Act Art.5 prohibition check; contextual integrity theory; LI academic critique and case law additions; and NIS2 assessment.

Bibliography and Legal References

A. Primary EU Legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation, GDPR/BDAR) [2016] OJ L 119/1.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences (Law Enforcement Directive, LED) [2016] OJ L 119/89. [NEW v2.0]

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) [2024] OJ L 1689.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act, DSA) [2022] OJ L 277/1.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) [2022] OJ L 333/80. [NEW v2.0]

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] OJ L 201/37.

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

B. Council of Europe Instruments

European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms), Rome, 4 November 1950, ETS No. 5.

Council of Europe, Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, amended and modernised 2018.

C. CJEU Case Law

CJEU (Grand Chamber), Judgment of 6 October 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (Schrems II).

CJEU (Grand Chamber), Judgment of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

CJEU, Judgment of 22 June 2021, Latvijas Republikas Saeima v NW (Latvijas Padomju), C-439/19, ECLI:EU:C:2021:504.

CJEU (Grand Chamber), Judgment of 4 July 2023, Meta Platforms Ireland and Others v Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537.

CJEU (Grand Chamber), Judgment of 7 December 2023, SCHUFA Holding AG v Datenschutzbehorde Hessen, C-634/21, ECLI:EU:C:2023:957.

CJEU, Judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein GmbH v Unabhangiges Landeszentrum fur Datenschutz Schleswig-Holstein, C-210/16, ECLI:EU:C:2018:388.

CJEU, Judgment of 29 July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, C-40/17, ECLI:EU:C:2019:629.

CJEU, Judgment of 16 December 2008, Tietosuojavaltuutettu v Satakunnan Markkinaporssi Oy and Satamedia Oy, C-73/07, ECLI:EU:C:2008:727. [NEW v2.0]

CJEU (Grand Chamber), Judgment of 24 November 2011, Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD), Joined Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777. [NEW v2.0]

CJEU, Judgment of 11 November 2020, Orange Romania SA v Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal, C-61/19, ECLI:EU:C:2020:901. [NEW v2.0]

CJEU, Judgment of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779.

CJEU, Judgment of 4 May 2017, Valsts policijas Rigas regiona parvaldes Kibberdatu koordinacijas birojs v Rigs, C-13/16, ECLI:EU:C:2017:336.

D. ECtHR Case Law

ECtHR (Grand Chamber), Judgment of 25 May 2021, Big Brother Watch and Others v United Kingdom, Applications Nos. 58170/13, 62322/14 and 24960/15.

ECtHR, Judgment of 9 April 2018, Benedik v Slovenia, Application No. 62357/14.

ECtHR, Judgment of 23 March 2021, Kharitonov v Russia, Application No. 10858/13.

E. EDPB and Supervisory Authority Guidance

Article 29 Working Party / European Data Protection Board, Guidelines on Data Protection Impact Assessment (WP248 rev.01), adopted 4 April 2017 (endorsed by EDPB).

European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted 20 October 2020.

European Data Protection Board, Guidelines 1/2024 on Processing of Personal Data Based on Legitimate Interest under Article 6(1)(f) GDPR, adopted 8 October 2024.

European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, adopted 13 April 2021.

European Data Protection Board, Guidelines 5/2020 on Consent under Regulation 2016/679, adopted 4 May 2020.

European Data Protection Board, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, adopted 18 June 2021.

Article 29 Working Party, Opinion 6/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP217), adopted 9 April 2014.

F. Standards

ISO/IEC 27001:2022, Information Security Management Systems - Requirements.

ISO/IEC 27701:2019, Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management.

ISO/IEC 27005:2022, Information Security, Cybersecurity and Privacy Protection - Guidance on Managing Information Security Risks.

ISO/IEC 23894:2023, Information Technology - Artificial Intelligence - Guidance on Risk Management.

ISO/IEC 42001:2023, Information Technology - Artificial Intelligence - Management System.

NIST Privacy Framework Version 1.0 (National Institute of Standards and Technology, 2020).

NIST AI Risk Management Framework 1.0 (National Institute of Standards and Technology, January 2023).

ENISA, Guidelines on Security Measures under Article 32 GDPR, 2020.

ENISA, AI Security Guidelines, 2023.

G. Academic Literature

Goddard, K., Roudsari, A., & Wyatt, J.C. (2012). Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators. Journal of the American Medical Informatics Association (JAMIA), 19(1), 121-127. [NEW v2.0]

Cummings, M.L. (2014). Man versus Machine or Man + Machine? IEEE Intelligent Systems, 29(5), 62-69. [NEW v2.0]

Kosta, E. (2013). Consent in European Data Protection Law. Martinus Nijhoff Publishers.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review, 79(1), 119-158. [NEW v2.0]

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press. [NEW v2.0]

Penney, J.W. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. Berkeley Technology Law Journal, 31(1), 117-182. [NEW v2.0]

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. Journalism & Mass Communication Quarterly, 93(2), 296-311. [NEW v2.0]

Zanfir-Fortuna, G. (2021). Towards "Operator Liability" in European Data Protection Law. International Data Privacy Law, 12(1), 25-44.

Editor
<<Main Editor>>

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

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

Disclaimer