TENACITy

Travel Intelligence Against Crime and Terrorism

Final Publishable Report

TENACITy Website:

https://tenacity-project.eu/

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Contents

Executive Summary 3
Glossary 4
Consortium Overview 5
Project Vision and Objectives 6
Field Overview, Challenges and Motivation 8
Purpose and Goals of the Travel Intelligence Governance Framework 9
TENACITy Achievements 10
From Data to Trust: Co-Designing Travel Security with Citizens and PIUs 11
What we did with citizens 12
What we learned from PIUs 12
What we delivered 13
What's next (beyond the project) 13
Technical Solutions 14
Risk Management Tool 14
Open-Source Intelligence (OSINT) Tool 14
Similarity Search Tool 14
Anomaly Detection Tool 15
Blockchain Tool 15
COPT Intelligence Automation Tool 15
TENACITy Training Platform 15
Piloting and Evaluation 16
Privacy, Ethical and AI-related Issues and Outcomes 16
Scientific Results 17
Published Scientific Publications 17
Navigating the challenges of passenger name record data and the way forward 17
Governance Framework in Travel Intelligence; The TENACITy Holistic Approach to Crime Prevention 18

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Using Blockchain to Secure Passenger Name Records and Effectively Protect Citizen Rights 18
Generating Realistic Passenger Name Records with Privacy Compliance for Security Analysis 19
Synthetic Passenger Name Record for Security Analysis 19
Pending / In Progress Scientific Publications 19
Potential Next Steps and Innovation Opportunities 20
Conclusions 21
Disclaimer 21
Project Information 22

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Executive Summary

This Final Publishable Report presents the main achievements and outcomes of the TENACITy project (Grant Agreement No. 101074048), a Horizon Europe initiative running from September 2022 to August 2025. The report is prepared for public dissemination and highlights key results relevant to stakeholders across the European security and travel intelligence ecosystem. The project brought together a multidisciplinary consortium of law enforcement agencies, research organisations, industry partners and technology providers to address pressing challenges in the governance and use of travel intelligence.

The project was conceived in response to the significant investments made by the EU and Schengen States in border management systems, alongside the persistent operational and regulatory challenges limiting their effective use. These challenges include fragmented approaches to Passenger Name Record (PNR) and Advance Passenger Information (API) systems, inconsistent data quality and insufficient interoperability all of which undermine the efficiency of security operations and the trust of citizens.

To overcome these obstacles TENACITy developed and demonstrated a comprehensive Travel Intelligence Governance Framework that combines innovative digital tools, interoperable IT architectures and advanced training curricula with legal, ethical and social acceptance frameworks. TENACITy aligned its solutions with European values and fundamental rights while supporting both operations and policymaking.

Over its three-year duration, TENACITy delivered tangible results in research, technological development and stakeholder engagement. It validated tools in real-world settings, enhanced cooperation among Member State authorities, promoted citizen trust through transparency and ethical safeguards and contributed to EU policy dialogue on responsible travel intelligence.

Through its collaborative approach and impactful results, TENACITy has strengthened Europe's capacity to prevent and investigate crime and terrorism, while ensuring that security measures respect privacy and societal values.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Glossary

- **API:** Advance Passenger Information
- **LEA:** Law Enforcement Agency
- **OSINT:** Open Source Intelligence
- **PIU:** Passenger Information Unit
- **PNR:** Passenger Name Record
- **RMF:** Risk Management Framework

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Consortium Overview

The TENACITy consortium brought together a diverse and complementary group of 17 partners from 10 European countries, ensuring a strong balance between operational expertise, scientific research, technological innovation and social sciences. This multidisciplinary composition was critical in addressing the project's ambitious objectives and in delivering practical, ethical and sustainable outcomes for European travel intelligence.

Law enforcement authorities and practitioners played a central role in grounding the project in operational realities. The Hellenic Police and the Cyprus Police both contributed through their Passenger Information Units, alongside the General Police Inspectorate of the Republic of Moldova, Aegean Airlines and the Customs Administration of the Czech Republic. Together, these partners ensured that TENACITy's tools and frameworks were directly applicable to the daily challenges of border management, policing and customs operations.

The consortium also integrated strong expertise in legal and ethical dimensions, provided by the Leibniz University of Hannover and social sciences perspectives, represented by Nutcracker Research Malta Ltd. These partners guaranteed that TENACITy's solutions respected regulatory requirements, safeguarded fundamental rights and contributed to building citizen trust in travel intelligence practices.

Research and academic excellence was ensured by the participation of leading institutions such as the Center for Security Studies (KEMEA), Transcrime – Università Cattolica del Sacro Cuore, the Institute of Communication and Computer Systems (ICCS) of the National Technical University of Athens and the University of Sheffield. Their contributions advanced methodologies in crime prevention, risk management and governance frameworks, while also validating the scientific underpinnings of the project's innovations.

Finally, the consortium benefited from a strong technological and industrial base. European Dynamics Luxembourg SA, as the project coordinator, worked alongside Ianus Consulting, Space Hellas and Hardware and Software Engineering to deliver interoperable architectures, innovative digital tools and integrated platforms to support both law enforcement authorities and policymakers.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

This unique combination of practitioners, legal and social experts, researchers and industry partners ensured that TENACITy's governance framework and technological solutions were operationally relevant, scientifically sound, ethically robust and technically innovative.

Figure 1 The TENACITy Consortium

Project Vision and Objectives

TENACITy was conceived with the vision of establishing a comprehensive Travel Intelligence Governance Framework that integrates technological, regulatory, ethical and social dimensions. The aim was to provide a holistic approach to crime prevention by strengthening intelligence and analytic capacities while ensuring legitimacy, trust and societal acceptance. This vision was implemented through six main pillars: analysing the state of play of passenger data usage in Europe, technically implementing and assessing the governance framework, developing innovative tools and business opportunities, liaising with and training partners and stakeholders, maximising demonstration and exploitation of results and securing acceptance through citizen engagement and legal assessment.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

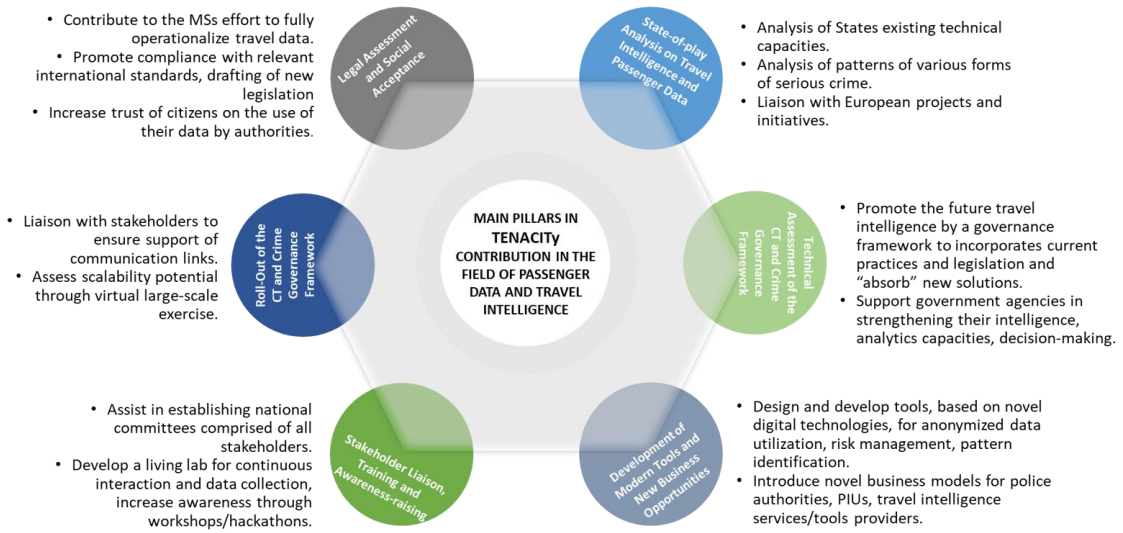

Figure 2 TENACITy Vision Elements

The project's science and technology objectives reflect this vision. TENACITy sought to enhance law enforcement capacity by delivering interoperable digital tools and architectures, strengthen cooperation and trust through governance mechanisms and provide advanced training curricula and living labs to practitioners. It also aimed to support policymakers with evidence-based insights into travel intelligence regulation and to facilitate trust-building between security actors and civil society. Validation activities in real-world settings ensured that the proposed solutions were tested under operational conditions, while exploitation planning focused on building on existing initiatives and paving the way for future services and business models. Together, these objectives ensured that TENACITy would not only deliver technical innovation but also create a sustainable impact across the full travel intelligence ecosystem.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

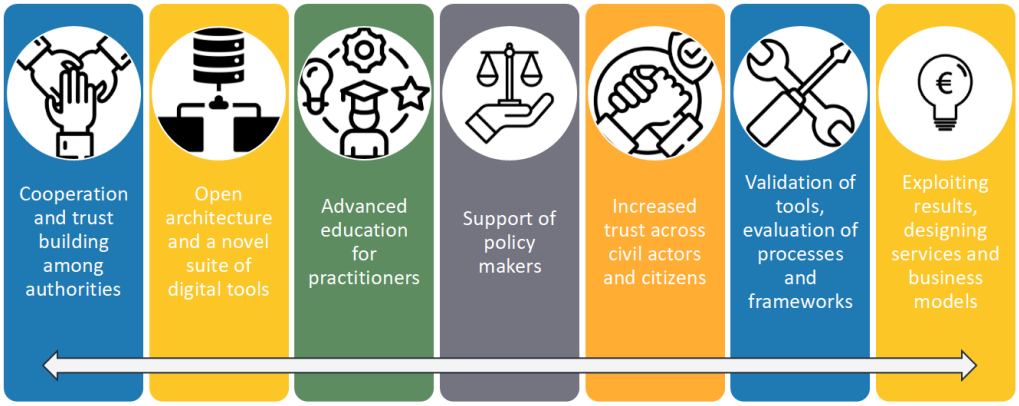

Figure 3 TENACITy Objectives

Against this background, TENACITy's vision and objectives are designed not only to advance research and technological innovation but also to directly serve its intended end-users. The primary beneficiaries are the Passenger Information Units (PIUs) established in each Member State of the European Union, which stand to gain from enhanced analytical, operational and governance capacities. Beyond PIUs, the project's outcomes are equally relevant to a wider community of actors involved in the transmission, use and standardisation of Advance Passenger Information (API) and Passenger Name Record (PNR) datasets and systems. These include border control authorities, law enforcement and intelligence agencies, customs administrations, as well as international organisations such as ICAO, WCO, IOM, INTERPOL and the UN Counter-Terrorism Centre. Air carriers and travel operators also represent essential stakeholders, since their role in data provision underpins the functioning of PIUs and the effectiveness of the broader travel intelligence ecosystem.

Field Overview, Challenges and Motivation

Over the last decade, the European Union and Schengen states have made substantial investments from the EU budget in information systems designed to address security and migratory pressures at external borders. These systems are used by a wide range of actors, including law enforcement agencies, customs, visa authorities and judicial services. Despite this substantial investment, however, persistent challenges limit the effectiveness of passenger data exploitation for crime prevention and border security.

Data quality and accuracy remain inconsistent across Member States, reflecting variations in training, methodologies and national legislative frameworks. The

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

implementation of Passenger Name Record (PNR) systems has been delayed in several countries and differences in regulatory approaches continue to hinder harmonisation. The absence of a common European platform for PNR has resulted in fragmentation, inefficiencies and underutilisation of the capabilities of EU-wide systems. In parallel, the increasing number of alerts and queries places pressure on available resources, raising concerns about sustainability and eroding citizen trust. Operational inconsistencies between PNR and Advanced Passenger Information (API) systems further complicate identity verification and limit the ability of authorities to identify security threats in a timely and reliable manner.

The motivation for TENACITy stemmed from these systemic shortcomings, which were also highlighted in reports from the European Court of Auditors. These reports emphasised that, despite major financial investments, Member States still faced difficulties in implementing interoperable PNR solutions and ensuring consistent use of passenger data across the EU. At the same time, low interoperability, fragmented legal frameworks and cultural differences across Member States created significant barriers to effective cooperation and trust building. The consortium recognised the need for a new governance model that could address these shortcomings and unlock the full potential of travel intelligence for security purposes.

Purpose and Goals of the Travel Intelligence Governance Framework

The purpose of the TENACITy Travel Intelligence Governance Framework was to develop a collaborative structure that optimises the governance of travel intelligence across Europe. It is designed to ensure the systematic improvement of procedures, processes and decision-making by bringing together operational, technical and legal dimensions under a common approach. The framework aims to facilitate the effective use of travel intelligence while addressing the key challenges faced by practitioners, such as data quality, interoperability and regulatory constraints. At its core, it establishes clear responsibilities (“whos”) and processes (“hows”), thereby streamlining governance and enhancing cooperation among partners and stakeholders. Importantly, the framework balances the need for operational efficiency with the protection of individual rights and privacy, ensuring that the use of travel data for crime prevention and security purposes remains both effective and socially acceptable.

The conceptual structure of this framework is illustrated in Figure 4, where communication forms the central element enabling continuous feedback between pre-

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101074048

assessment, management, characterisation and evaluation and appraisal. This cycle highlights the framework's adaptability, designed to evolve with operational needs, regulatory requirements and societal expectations.

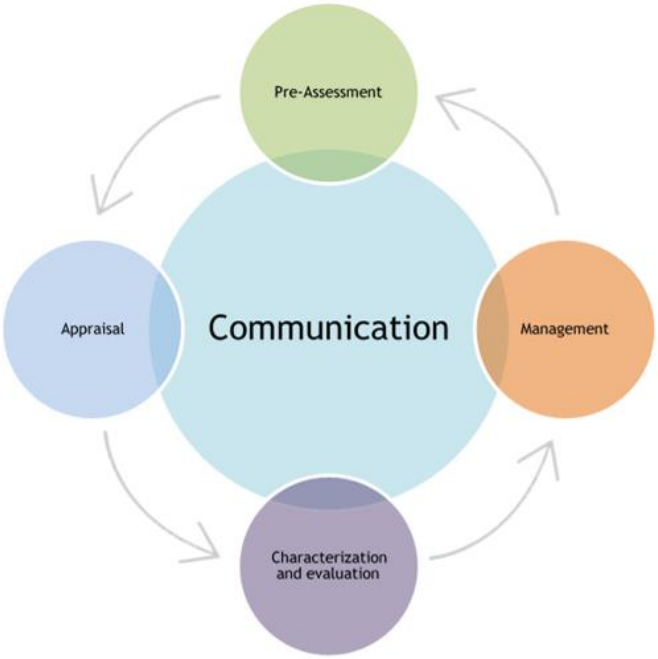

Figure 4 Travel Intelligence Framework (Purpose & Goals)

TENACITy Achievements

Over its three-year implementation, TENACITy delivered a set of concrete achievements that demonstrate the added value of its holistic Travel Intelligence Governance Framework. These achievements reflect both the technical developments and the active involvement of partners and stakeholders throughout the project's lifecycle.

First, TENACITy successfully designed and validated its Travel Intelligence Governance Framework, supported by a suite of innovative tools and methods tailored to the needs of Passenger Information Units (PIUs) and other security authorities. This framework addressed operational, legal and ethical dimensions, ensuring that technological

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

advancements were accompanied by safeguards for transparency, accountability and citizen trust.

Second, the project advanced the understanding of criminal organisations' modus operandi through the analysis and generation of PNR-related datasets. These insights enabled more effective detection of cross-border crime and terrorism patterns, while also highlighting the challenges of data quality and interoperability across Member States.

Third, TENACITy placed a strong emphasis on stakeholder engagement, training and trust building. Through dedicated workshops, pilot demonstrations and living labs, the project created opportunities for law enforcement agencies, policymakers and civil actors to exchange knowledge, test solutions in realistic environments and co-design practices that respect fundamental rights.

Finally, the project conducted an in-depth assessment of PIU operations and travel intelligence sources, identifying key operational gaps and opportunities for improvement. This ensured that the proposed solutions were not only innovative but also practical and adaptable to the real needs of end-users.

Together, these achievements confirm TENACITy's contribution to reinforcing the security ecosystem in Europe by enhancing travel intelligence, strengthening cooperation among stakeholders and fostering trust between authorities and citizens.

From Data to Trust: Co-Designing Travel Security with Citizens and PIUs

Modern travel security increasingly relies on the use of data and advanced technology, including AI. Public confidence rests on two things: clear safeguards and clear explanations. TENACITy brought citizens and law-enforcement practitioners (PIUs) into the process so the solution would address real concerns, real workflows and real constraints. The project ran a series of workshops with citizens in three EU countries. In parallel, interviews with national PIUs explored operational fit, adoption conditions, and barriers. Together, these two strands informed the development of the solution and provided guidance to PIUs on how to communicate transparently with the public to boost perceptions of legitimacy and competence, and promote engagement.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

What we did with citizens

We held 18 in-person workshops in Athens, Nicosia and Prague, speaking with a broad mix of citizens about (1) what happens to their passenger data today and (2) how they would feel about a new, PIU-run data system which used PNR to tackle cross-border crime. We also tested short, plain-language messages designed to explain the purpose of the system, the safeguards included in its design, and the role of human oversight. During the sessions we explored what information people need to feel safe and fairly treated. To help bring the discussion to life, research materials displaying information and possible messages that could be used to explain the role of the technology, were used. These were prepared centrally and translated into the local languages. The workshops were carried out in two waves. The first wave mapped citizens' baseline awareness and concerns about PNR. The second examined reactions to the proposed system and the likely influence of different message types or perceived legitimacy and feelings of safety and trust.

Most participants accepted the *principle* of using passengers' travel data to prevent serious crime. This was dependent on proportionate use, time-limited retention, and being subject to human and independent oversight. People wanted to know exactly what data is used, by whom, for how long, and what to do if something goes wrong (appeal, correction). Jargon reduced trust, and layered information (a short explainer with optional detail) worked best. Across cities, the privacy/data-protection framing consistently reassured more than other framings. These insights fed into a set of guidelines for citizen-facing communications to be used by LEAs planning to roll out TENACITy.

What we learned from PIUs

To complement citizen input, we interviewed four national PIUs (Belgium, Cyprus, Greece, UK) whose staff had used the prototype at the Living Lab. They described difficulties in their current operational realities (such as, a lack of interoperability of multiple tools, manual steps, and data-quality issues) and the perceived value of anomaly detection and OSINT integration. The key elements that emerged as making TENACITy usable and appealing were: modularity, interoperability, and explainable, auditable automation with a clear human-in-the-loop. Legal and policy constraints (including rules on AI use and hosting) vary by country and could delay adoption unless planned for early.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

PIUs also highlighted the burden of manual processes (such as, data validation, case-management integration, OSINT checks) and the cost of non-standard data formats sometimes used across modes and carriers, and which often create bottlenecks and increase error risk. Addressing these issues raises the appeal of any tool that can handle variability while keeping robust audit trails.

What we delivered

- Guidance on meeting PIU requirements: The PIU interview findings fed into the later development of TENACITy and complemented its strong governance and communications approach, underscoring the need for early integration planning, explainability, and documented human overview.
- Synthesis of PIU needs for roll-out: A concise summary of what PIUs would require if considering TENACITy was produced to guide future roll-outs: Key requirements are modularity, interoperability and explainability to inform governance and communications as systems evolve.
- Citizen-centred guidance for LEAs: We turned citizen feedback into a set of guidelines that will help PIUs explain, in plain language the: purpose, in-built data protections, human oversight, independent checks, and routes to complain or appeal.
- Recommendations for public messaging: As revealed by the research, the messages that perform best emphasise privacy and data-protection safeguards, backed by a straightforward description of personal data retention, access controls, and redress.

What's next (beyond the project)

The findings from the research give a clear direction on how to maximise the benefits of TENACITy. On the one hand, a modular and customisable deployment model will benefit PIUs, while layered, plain-language citizen-facing communications will maintain perceptions of legitimacy, transparency and accountability.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Technical Solutions

TENACITy developed a suite of advanced tools to implement the Travel Intelligence Governance Framework, supporting the prevention and investigation of serious crime and terrorism. These interoperable tools were co-designed with Passenger Information Units and security practitioners to ensure alignment with EU ethical and legal standards.

Risk Management Tool

The Risk Management Tool parses incoming PNR data and serves it to the other TENACITy tools. It facilitates the creation of Risk Assessments based on available PNR data and dynamically evaluates traveler risk scores. It connects to other TENACITy tools to enhance the results of the Risk Assessments and facilitates the exchange of PNR requests between PIUs. The Risk Management Tool operationalises the Risk Management Framework (RMF) developed by Transcrime – the Joint Research Centre on Innovation and Crime at Università Cattolica of Milan. This framework is grounded in criminological literature, official reports and case studies, complemented by a dedicated survey of Passenger Information Units (PIUs) and Law Enforcement Agencies (LEAs). The RMF translates recurrent modi operandi, routes and criminal actor typologies into observable risk indicators and individual risk scores, supporting early, evidence-based prioritisation while preserving fundamental-rights safeguards and avoiding fully automated decisions.

Open-Source Intelligence (OSINT) Tool

Complementing the RMT, the Open-Source Intelligence Tool (OSINT) incorporates crawling pipelines that enable extensive searches across multiple environments. It is capable of analysing diverse open and controlled information sources while respecting privacy and legal frameworks. The tool also supports restricted online environments searches, monitoring of communication platforms and network discovery. In close collaboration with PIUs, risk terms have been defined and categorised according to the project's use cases, including drug trafficking, terrorism and human trafficking.

Similarity Search Tool

The Similarity Search Tool facilitates the identification of individuals whose identity may be either accidentally or deliberately obfuscated. It calculates the likelihood that a Passenger Name Record (PNR) corresponds to the same individual, or to a similar type of individual, as specified in a particular query. By doing so, the tool enhances the searches and risk assessments conducted through the Risk Management Tool, improving the accuracy and reliability of traveler identification.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Anomaly Detection Tool

In parallel, the Anomaly Detection Tool applies clustering techniques to make use of distance metrics for modeling traveler or data patterns. It identifies anomalies by assessing the distance between individual instances and their proximate clusters, thereby detecting unusual or suspicious behaviors. This approach enables the early identification of potential risks or irregularities in passenger data, strengthening the overall reliability of the risk assessment process.

Blockchain Tool

The Blockchain Tool was developed as an alternative communication channel to existing secure data exchange systems, enabling the secure exchange of Passenger Name Record (PNR) data as well as other types of data and metadata beyond passenger movement. Developed on Hyperledger Fabric, the tool combines blockchain technology with private data storage in a single solution. Its design ensures inherent security through the use of certification authorities and operates within a permission-based network, where all participating parties are known to each other. The solution has been tested in enterprise environments, confirming its robustness and suitability for operational use.

COPT Intelligence Automation Tool

The COPT Tool was designed to support intelligence automation by leveraging machine learning models trained on historical data. It facilitates the generation of leads from incoming data, offering suggestions for similar or associated individuals while integrating explainability traits to ensure transparency. The tool includes mechanisms for human or manual review, allowing analysts to set thresholds for lead designation, dismiss leads, or promote them to Subjects of Interest (SOIs), thereby converting leads into cases. Analysts can also dismiss SOIs, select suggested similars or associates to strengthen case files and ultimately decide to close cases as either conclusive or inconclusive. This structured process enhances efficiency in handling intelligence data while ensuring human oversight remains central.

TENACITy Training Platform

In addition to the toolset, the TENACITy training platform was developed to provide practitioners with both theoretical and practical knowledge essential for the effective use of travel intelligence in crime prevention and security operations. The programme offered structured modules covering the legal foundations of travel intelligence, the Travel Intelligence Governance Framework and the integration of citizens' perspectives into operational practices. In addition to the conceptual modules, trainees were

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

introduced to the TENACITy suite of tools, including the Pattern Identification Tool, Risk Management Tool, OSINT modules, the Blockchain-based data exchange solution and AICOPT. These sessions enabled participants to gain hands-on experience with the technologies and to better understand their role in identifying risks, managing data and enhancing decision-making. The training process also included an evaluation component, assessing performance and verifying the achievement of defined learning objectives. This ensured that the acquired knowledge was effectively consolidated and that the skills gained were directly applicable to the operational contexts of Passenger Information Units and law enforcement authorities.

Piloting and Evaluation

As the leader of TENACITy's piloting activities, KEMEA played a pivotal role in bringing these technical innovations to life through real-world demonstrations and operational validation. Two full-scale pilot exercises and the Final Event enabled end-users across Europe to test the integrated toolset in realistic scenarios. KEMEA oversaw the design and execution of the evaluation methodology, supported participants with targeted training, and implemented structured feedback mechanisms to refine system usability and performance. The successful completion of these pilots marked a major step forward in demonstrating the operational readiness and scalability of TENACITy's solutions across different national contexts.

Together, these tools reflect TENACITy's holistic approach to travel intelligence, combining technological innovation with legal, ethical and social safeguards. Their integration under the Governance Framework demonstrates how Europe can enhance interoperability, strengthen operational capacities and maintain citizen trust in the responsible use of travel data.

Privacy, Ethical and AI-related Issues and Outcomes

A legal and ethical framework was developed to cater to the project's lifecycle, consisting of a tripartite structure to provide guidelines on activities with legal and ethical impacts, monitor implementation of any requirements or recommendations, as well as an Ethics Advisory Board (EAB) to supervise relevant matters. This structure led to the identification of relevant stakeholders, and the design and administration of templates for informed consent.

A thorough evaluation of the impact of the legal and ethical developments around AI was conducted, given that the project involved the development of AI systems. Key

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

instruments such as the AI Act, GDPR, and the Ethics Guidelines for Trustworthy AI were identified and analyzed to elicit requirements for the tools' development. A privacy-by-design and ethics-by-design approach was adopted to ensure that relevant requirements were incorporated into the system's architecture.

Furthermore, an impact assessment of the AI tools was conducted to ensure they align with EU fundamental human rights and values. Each AI-related tool was assessed in terms of benefits and risks, and mitigations. Overall, key policy recommendations were made to the relevant stakeholders, including the European Commission, on how to bridge the gaps in this area of innovative research and development.

Scientific Results

During the course of the TENACITy project, several scientific papers and related research outputs were produced, contributing to the advancement of knowledge in travel intelligence, data governance, and privacy-preserving technologies.

Published Scientific Publications

Navigating the challenges of passenger name record data and the way forward

Aposkiti C and Makri F. Navigating the challenges of passenger name record data and the way forward [version 2; peer review: 1 approved, 4 approved with reservations, 1 not approved]. Open Res Europe 2025, 4:168 (https://doi.org/10.12688/openreseurope.18037.2)

Background

The TENACITy EU-funded project investigates the multifaceted challenges surrounding the utilisation of Passenger Name Record (PNR) data following the implementation of the PNR Directive (EU) 2016/681, which marks a significant shift in EU air travel intelligence.

Methods

This study employed a combination of research and survey methodologies to gather data from various stakeholders involved in the implementation of the PNR Directive. The survey focused on identifying the key obstacles faced by Passenger Information Units (PIUs), including the absence of standardised practices and issues of data quality.

Results

The findings highlight two primary obstacles confronting PIUs: the lack of standardised practices among stakeholders and the poor quality of PNR data. Additionally, fragmented implementation

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

and regulatory barriers were identified as significant hindrances to the optimal utilisation of PNR data for counterterrorism and crime prevention efforts.

Conclusions

Addressing these challenges requires nuanced solutions, with technological tools presenting potential remedies to operational constraints. There is a collective call for mandating specific data elements to enhance the effectiveness of PNR data utilisation. This paper provides insights and recommendations to enhance PIUs' capabilities, contributing to the ongoing discourse on EU travel intelligence.

Governance Framework in Travel Intelligence; The TENACITy Holistic Approach to Crime Prevention

Panos Karaivazoglou, Rodoula Makri, Christoforos Antoniou, George Boultadakis, "Governance Framework in Travel Intelligence; The TENACITy Holistic Approach to Crime Prevention", announced and published at the Proceedings of the Research and Innovation Symposium for European Security and Defence 2024 (RISE-SD 2024), Chalkidiki, Greece, 16-17 October 2024, Procs pp. 41-43, https://rise-sd2024.eu/

https://rise-sd2024.eu/wp-content/uploads/2024/10/RISE-SD_2024-Online_Proceedings-draft.pdf

Using Blockchain to Secure Passenger Name Records and Effectively Protect Citizen Rights

M. Koutenský, V. Veselý, M. Perešíni, D. Dolejška and J. Pluskal, "Using Blockchain to Secure Passenger Name Records and Effectively Protect Citizen Rights," 2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Berlin, Germany, 2024, pp. 1-10, https://doi.org/10.1109/BRAINS63024.2024.10732767

Abstract:

Passenger Name Records (so called PNR) collected by airlines and processed by Passenger Information Units (dedicated police task force), are critical data in the prevention and successful investigation of terrorism, drug smuggling, human trafficking and other serious crimes. This work addresses the challenges of building a blockchain-based, tamper-proof system for PNR data exchange between different Passenger Information Units. Utilizing Hyperledger Fabric, we propose a decentralized architecture that ensures data confidentiality, traceability, and non-repudiation in order to maintain the chain of custody. Our solution includes a private data collection mechanism and an offchain storage system to manage sensitive information securely. The resulting design and implementation are incorporated into the TENACITy project platform and further integrated with its other modules to use travel intelligence data in the fight against crime. The blockchain subsystem facilitates a secure, auditable exchange of PNR data, with the

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

key benefit being compliance with European Union regulations on the protection and retention of personal data. This paper contributes to the field by demonstrating the practical application of blockchain technology in a sensitive data exchange scenario, offering insights into system design, implementation challenges, and potential future enhancements.

Generating Realistic Passenger Name Records with Privacy Compliance for Security Analysis

Fadlian, M. F., Ireson, N., & Lanfranchi, V. (2025). Generating Realistic Passenger Name Records with Privacy Compliance for Security Analysis. Proceedings of the International ISCRAM Conference. https://doi.org/10.59297/mbf3dq94

Passenger Name Record (PNR) data is essential for transportation analysis and security research, particularly in surveillance and threat detection. However, stringent security and privacy concerns limit access to real PNR data. This study presents a methodology for generating synthetic PNR data that not only replicates statistical properties but also reconstructs passenger social networks, models travel behaviours and preserves individual travel histories for security and mobility analysis. Our approach generates detailed, individual-level data—including passengers, bookings, and flights—while maintaining spatial, temporal, and chronological consistency to ensure realistic movement patterns while upholding privacy. This methodology offers a privacy-preserving alternative for transportation security and behavioural research, expanding access to high-quality data for future studies.

Synthetic Passenger Name Record for Security Analysis

Fadlian, M. F., Ireson, N., & Lanfranchi, V. (2025). Synthetic Passenger Name Record for Security Analysis (1.86) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.16739439

This dataset contains synthetic Passenger Name Record (PNR) data simulating international air travel bookings across countries in the Schengen region during 2019. It includes over 400,000 synthetic passengers and 20,000+ flights formatted in XML following the IATA PNRGOV v16.1 schema.

The data supports research in air travel modeling, mobility analysis, and aviation security, and is fully privacy-preserving. See the accompanying technical documentation and paper for full methodology and known limitations.

Pending / In Progress Scientific Publications

In addition to the peer-reviewed and publicly available publications listed above, several manuscripts are currently in preparation or under review, reflecting the ongoing scientific dissemination efforts of the TENACITy consortium. These works further develop the project's key findings, covering topics such as AI-driven risk assessment, federated learning for secure data sharing, citizen trust in data-driven border security, and the legal-ethical frameworks underpinning travel intelligence governance. Once published, they will consolidate TENACITy's

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

contribution to advancing responsible, privacy-aware, and operationally effective approaches to European travel intelligence.

1. Using Blockchain to Secure Passenger Name Records and Effectively Protect Citizen Rights: Director's Cut, ACM journal Distributed Ledger Technologies: Research and Practice (DLT)
2. Oracleboros: Reusing Hyperledger Fabric Mechanism to Provide Oracle Functionality, The 7th International Conference on Blockchain Computing and Applications (BCCA 2025)
3. Nwankwo, Iheanyi Samuel and Seckelmann, Margrit and Corrales Compagnucci, Marcelo and Karaivazoglou, Panos and Makri, Rodoula, "Traversing EU Pnr Challenges: Balancing Compliance and Innovation in Travel Intelligence", submitted for publication (29 pages, February 2025) in Journal on "Computer Law & Security Review: The International Journal of Technology Law and Practice", ScienceDirect Elsevier. Currently is under review. A preprint is available on SSRN: https://ssrn.com/abstract=5212425 or http://dx.doi.org/10.2139/ssrn.5212425 , where it has reached the Top10 of paper downloads of SSRN's Top Downloads list up to 31 May 2025.
4. Living Labs as catalysts for experiential learning in law enforcement training: Insights from the TENACITy Project

Potential Next Steps and Innovation Opportunities

The development of TENACITY demonstrates clear potential to strengthen travel intelligence services for Passenger Information Units (PIUs). By enhancing the way travel data is enriched, analysed and operationalised, TENACITY provides a foundation for more accurate and efficient decision-making in the management of cross-border threats.

A natural next step is the deeper integration of heterogeneous data sources into PIU workflows. Combining PNR and API data with open-source intelligence, darknet monitoring and social media analysis can give PIUs a more complete picture of individuals and networks of interest. Advanced correlation models and multilingual text analysis could further support the identification of hidden connections across jurisdictions, allowing PIUs to spot risks that traditional systems may overlook.

TENACITy also opens innovation opportunities in risk assessment. By embedding adaptive learning into risk models, PIUs could benefit from continuously improving accuracy informed by real operational feedback. This would support the expansion of risk scoring beyond narcotics into areas such as terrorism financing, trafficking in cultural goods or cyber-facilitated crime. Moving towards predictive models would shift PIU services from primarily reactive assessment to proactive early-warning capabilities.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

At the same time, the project highlights the importance of privacy, security and trust in travel intelligence. Future developments could explore privacy-enhancing technologies, such as federated learning or encryption-based approaches, that allow information sharing and cross-border cooperation without compromising data protection standards. This would enable PIUs to strengthen collaboration with partners while remaining compliant with European legal and ethical frameworks.

Finally, innovation opportunities lie in making PIU services more user-centric. By embedding TENACITy tools into intuitive dashboards, offering prioritised alerts and providing tailored training environments, the system can better match operational realities. Continuous feedback between analysts and developers will ensure that tools remain aligned with the evolving needs of PIUs.

In this way, TENACITy is positioned not only as a proof-of-concept but as a scalable capability that can modernise PIU travel intelligence services. Its further development can help authorities across Europe achieve a more proactive, data-driven and trusted approach to cross-border security.

Conclusions

Over its three-year implementation, TENACITy has demonstrated that innovation in travel intelligence can advance operational efficiency without compromising European values of privacy, ethics, and transparency. The project successfully delivered a comprehensive governance framework, validated a suite of interoperable tools, and fostered collaboration between law enforcement, policymakers, researchers, and citizens. Its results have contributed not only to enhanced analytical and risk-assessment capabilities for Passenger Information Units but also to the broader policy dialogue on responsible data use in security operations.

As the consortium moves beyond the project's formal end, TENACITy leaves behind a scalable, evidence-based foundation for future European initiatives in secure data governance, cross-border cooperation, and citizen-trusted digital security ecosystems ensuring that the benefits of technological progress continue to serve both security and fundamental rights across Europe.

Disclaimer

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

Project Information

- **Project Website:** https://tenacity-project.eu/
- **LinkedIn:** https://www.linkedin.com/company/tenacity-horizoneu/about/
- **X:** https://x.com/TenacityProject
- **Vimeo:** https://vimeo.com/tenacityprojecteu

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048