EUROPOL

INNOVATION LAB

**Application to present at**

# Europol Industry and Research Days

**25-26 February 2026**

## 1. Aim of the Event:

Technology offers new opportunities throughout society but also makes it easier for criminals to commit crimes and to remain anonymous when doing so. The European Union Agency for Law Enforcement Cooperation (Europol) wants to offer the law enforcement community the opportunity to use emerging technologies and to acquire new skills and develop alternative investigative techniques to deal with evolving threats. However, the law enforcement community faces challenges in understanding what is currently available, particularly in the context of rapidly advancing artificial intelligence, quantum technologies, and sophisticated digital crime methodologies.

Europol confirms its determination to remain at the forefront of law enforcement innovation and research, as part of its broader efforts to improve the efficiency of law enforcement operations, as stated also in the Europol Strategy adopted in June 2023[1].

In order to achieve this strategic objective, proactive engagement and close collaboration with the private sector, academia and research institutes is considered essential. Europol organises a dedicated series of events to set a fair and transparent framework and create a level playing field for private parties[2]: the **Europol Industry and Research Days**. The second successful edition took place in February 2025[3].

[1] https://www.europol.europa.eu/publications-events/publications/europol-strategy-delivering-security-in-partnership#:~:text=Europol's%20strategy%2C%20'Delivering%20Security%20in,and%20the%20war%20in%20Ukraine.

[2] Private parties encompass entities and bodies established under the national law in particular companies and firms, business associations, non-profit organisations, research institutions and other legal persons that are not international organisations.

[3] https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025

**On 25-26 February 2026**, the Europol Innovation Lab will organise the third edition of Europol Industry and Research Days and invite selected private parties to present their products/services. The event will take place in person **at Europol's premises in The Hague, The Netherlands**.

**2. Why participate in the Event:**

The Event is free of charge, and it intends to bring together Europol staff, law enforcement practitioners from EU Member States and third countries[4], and other stakeholders invited by Europol, as well as companies, and research and technology institutes with the following objectives:

- Informing Europol staff and national law enforcement practitioners about the latest technological advancements available in the security market, with particular focus on AI-enhanced capabilities, quantum-resistant solutions, and next-generation digital forensics tools.
- Increasing research and innovation actors' understanding of investigative use cases for state-of-the-art and emerging technologies, particularly in multi-modal data processing, encrypted communications access, and synthetic content detection.
- Increasing participants' understanding of solutions for compliance needs, e.g., personal data protection, fundamental rights, artificial intelligence (AI) legislation, quantum-safe cryptography standards, and ethical/transparency considerations in automated evidence processing.

The upcoming edition will build upon the successes of previous events by introducing new formats to stimulate collaboration, discussion, and practical demonstration. Companies and institutes attending will not only present their latest technological solutions but also participate in hands-on sessions, allowing law enforcement professionals to directly experience the usability and effectiveness of proposed tools. The event's agenda is carefully structured to facilitate both formal presentations and informal exchanges, maximising opportunities for learning and partnership.

In addition to promoting knowledge transfer, Europol aims to bridge the gap between innovation and operational needs, enabling stakeholders to co-create solutions that directly address evolving crime trends. Special attention will be given to solutions that demonstrate robust compliance with EU standards, especially in areas of privacy, ethics, and transparency, ensuring that technological advancements align with core values and legal obligations in European law enforcement.

[4] https://www.europol.europa.eu/partners-collaboration/agreements

**3. Who should participate in the Event:**

The Event targets companies and research and technology organisations (RTOs) that offer technical solutions, tools, methodologies and processes related to key challenges faced by European Law Enforcement Agencies (LEAs), with particular emphasis on sovereign technology solutions and EU-compliant frameworks.

**ANNEX** includes a list of topics intended to guide and inform applicants about the areas of greatest interest to Europol and to LEAs. These topics are related to the capability gaps identified at EU Member States' level, compiled by the Europol Innovation Lab in cooperation with Europol and national experts, including via the European Clearing Board (EuCB), and informed by the High-Level Group on lawful data access recommendations.

Please note that priority will be given to the topics mentioned in ANNEX. However, applicants are allowed to propose topics other than those mentioned in ANNEX. Europol reserves the right to reject applications which do not align with the topics covered by ANNEX at its own discretion.

Interactive, creative solutions that participants can manoeuvre or interact with are highly welcome, particularly those demonstrating real-time processing capabilities and explainable AI decision-making.

To encourage meaningful engagement, the Event will also feature networking opportunities designed to foster collaboration between technology providers, researchers, and law enforcement professionals. Participants will have the chance to connect with peers, exchange ideas, and explore potential partnerships that could drive forward innovation in the security sector. Additionally, a series of breakout sessions and interactive panels will address the practical challenges of deploying advanced technologies in law enforcement environments, providing an open forum for discussion and knowledge sharing.

**Only proposals for solutions at TRL 8 or above will be reviewed[5].**

**4. How to submit your interest in the Event:**

To ensure only the most advanced and practical innovations are showcased, proposals must clearly demonstrate the readiness of the solution for real-world deployment, as indicated by their Technology Readiness Level (TRL) of 8 or higher. Applicants should provide comprehensive documentation of their solution's capabilities, previous deployment cases, and compliance with relevant EU regulations. Emphasis will be placed on solutions that not only address the outlined challenges but also offer transparency, user-friendliness, and measurable improvements for end-users within law enforcement contexts.

[5] TRL 8 is the stage where a technology is fully developed, tested, and qualified in its final form under expected conditions, but it has not yet been deployed in an actual operational environment. TRL 9 is the stage where the technology has been proven in an operational environment. Please see the General Annexes v2.0 to the Horizon Europe Main Work Programme 2023-2025: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-13-general-annexes_horizon-2023-2024_en.pdf

Interested organisations need to submit a Request to Participate by ~~5~~ **12November 12:00 AOB**. via the following link:

https://ec.europa.eu/eusurvey/runner/35924acf-7992-dd39-e477-f156263c18a3

**5. Admission to the Event:**

The evaluation process will be conducted in two stages.

In Stage 1, all submitted Requests to Participate will be reviewed and assessed by a Panel composed of Europol staff, taking into consideration the following criteria:

1. Alignment of the proposed presentation with the selected topics referenced in ANNEX;
2. Innovative nature of the product, with particular consideration for EU sovereignty and fundamental rights compliance;
3. Suitability of the proposed presentation for the needs of European Law Enforcement Agencies as users of technology with a strong interest in compliance with emerging EU regulations (AI Act, Data Act, NIS2 Directive);
4. Maturity level of the proposed product (TRL 8 or above);
5. Demonstrated effectiveness in operational law enforcement environments.

[6]Each member of the Panel will sign a declaration of absence of conflict of interest and of confidentiality.

The Panel will evaluate and score each Request to Participate individually against every criterion. A first shortlist of Requests to Participate will be drawn and pre-selected private parties who pass the minimum admissible score (of 60% per criterion) will be invited to participate in the second stage. The Request to Participate must include information on the private party and its key office holders/shareholders. This is required in order to conduct basic checks: Europol reserves the right to check that none of the participating private parties are subject to EU restrictive measures adopted under Article 29 of the Treaty on the European Union (TEU) or Article 215 of the Treaty on the Functioning of the EU (TFEU). In addition, Europol may exclude or score lower Requests to Participate where there are substantiated concerns about the company's standing (e.g., EU sanctions in place impacting on a company or its key office/shareholders).

By ~~19~~ **26 November 2025**, Europol will communicate the outcome of the first evaluation stage to the relevant private parties. Europol's intention is to invite up to 30 private parties to the second evaluation stage.

In Stage 2, pre-selected private parties will be invited to participate in interviews, allowing for a more in-depth discussion of their proposals and giving the Panel an opportunity to address any questions or clarifications regarding technical implementation, compliance frameworks, and operational deployment scenarios. A final total score will be given after Stage 2 to the private parties that are eventually selected. By **19 December 2025**, Europol will communicate the outcome of the second evaluation stage to the relevant private parties.

[6] For example, in relation to data protection, respect for fundamental rights, ethics, transparency and explainability.

Europol's intention is to invite up to 24 private parties[7] which have received the highest total scores after Stage 2 to participate at the February 2026 edition of the Europol Industry and Research Days. Selected private parties will need to confirm participation by **21 January 2026, 24:00 AOB**. In the absence of confirmation, Europol may invite the next private party in line on the admission list.

Your organisation may request additional information about the non-admission of your Request to Participate **by ~~26 November~~ 3 December 2025 13:00 AOB for Stage 1** and **by 02 January, 13:00 AOB for Stage 2**. Upon request to Innovation-Lab@europol.europa.eu, Europol will set up a Review Committee composed of individual staff members not present on the initial Panel. The Review Committee will re-assess your Request and take a final decision on inclusion/non-inclusion, providing its reasoning, **by ~~3~~ 10 December for Stage 1 and by 16 January for Stage 2.**

The admission of your Request to Participate and the presentation of your proposal at the Industry and Research Days shall not be understood as leading to an acquisition process or a purchasing phase. The aims of the Event are broad, and this Event does not alter the financial rules governing acquisitions of technology or services. Neither Europol nor any other contracting authority commits to conduct any public procurement procedures because of the Industry and Research Days. While the objectives of the Event lend themselves to broad participation, and no specific procurements are planned as a result, it should be noted that the participation of third country entities in public procurement procedures is regulated by law: for some national authorities third country participation is foreseen under WTO rules or other international rules, whereas for others and Europol third country participation is an exception.

## 6. Final remarks about the Event:

A provisional agenda, with any logistics details, will be provided to the selected private parties **by 23 January 2026**.

Presentations by the invited organisations (slides, pitches and flyers) are due on **Thursday 29 January 2026 AOB** to Innovation-Lab@europol.europa.eu. Please note that last-minute changes will not be accepted for organisational reasons.

Europol will organise preparatory meetings with invited speakers in January 2026 to collect presentations, clarify any final questions and ensure that the guidelines set in this document are understood and respected.

Europol reserves the right to live stream parts of the event (plenary sessions) via Webex to an invited audience of law enforcement authorities and Europol staff.

Participation in the Event by the selected private parties will be at their own expense. Europol will not reimburse any related costs.

[7] Europol reserves the right to increase or decrease the total number of companies invited to the event.

**Communication**

When making public statements (including on social media) regarding this Event (and the participation of a private party at the Event), participants must refrain from implying any endorsement by Europol (or by any other third party) of the private party or any of its products/services. Use of Europol's logo requires advance permission in writing from Europol.

**Transparency statement**

Any documentation shared or correspondence with Europol in relation to the Event, including submitted Requests for Participation, is subject to the rules on public access to documents held by EU bodies. While there are possible exceptions to the release of documents under these rules (e.g., redactions needed for protection of personal data or commercial interests including intellectual property), Europol is keen to ensure transparency towards the public in relation to the Event. Therefore, at least the presentations should refrain from including any personal data, trade secrets or commercially sensitive information: This statement holds for any material provided to participants insofar as they are provided to Europol (e.g., a Europol participant).

As stated above, Europol staff members participating in the evaluation Panel are required to sign a declaration on the absence of conflicts of interest and confidentiality. In addition, members of the Evaluation Panel and other Europol staff participating in the Event are not allowed to (i) discuss any future purchasing needs other than in very general terms; (ii) enter into a detailed dialogue about a particular product/service/technology with representatives from presenting private parties if they would envisage being involved as an evaluation member in any Europol procurement procedure launched in the 12 months after the Event. Europol is under an ongoing obligation as regards identifying and avoiding conflicts of interest but considers that the mere participation of a Europol staff member in a demo would not of itself constitute a conflict of interest in the absence of other indications.

**Personal Data Privacy Statement**

Any personal data provided in relation to the organisation of the Europol Industry and Research Days will be handled by Europol in accordance with the provisions of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC applicable to all administrative personal data held by Europol in accordance with Article 27a (1) of the Europol Regulation.

**PUBLIC ACCESS REQUEST:**

Following the event, please be aware that any documents produced may be subject to public access requests under Regulation (EC) No 1049/2001, which establishes the right of EU citizens and residents to access documents of EU institutions and agencies.

However, given that these events focus specifically on addressing law enforcement needs rather than public dissemination, selected participants retain full control over their materials and may decline sharing their presentations or provide modified versions suitable for public release.

Similarly, participants may opt to exclude their names (individual or company) from any publicly communicated agenda or documentation.

Europol will handle any access requests within 15 working days and will consult participants prior to any document disclosure to ensure their confidentiality preferences are respected

https://eur-lex.europa.eu/eli/reg/2001/1049/oj/eng

For any clarification or questions, please write to Innovation-Lab@europol.europa.eu

# Annex – LIST OF TOPICS

## 1. Lawful Data Access Solutions

**Context**:

EU law enforcement faces critical challenges accessing digital evidence due to fragmented systems, incompatible data formats, limited processing capabilities, and evolving encryption technologies. Solutions must enhance investigative efficiency whilst maintaining strict legal frameworks, fundamental rights protection, and proportionality principles.

**Innovation Areas:**

- Unified Multi-Source Evidence Platforms: Integrated solutions enabling simultaneous collection and analysis from diverse digital sources including mobile devices, computers, IoT systems, vehicles, cloud storage, and emerging technologies with standardised interfaces and European law enforcement workflow compatibility.
- Automated Evidence Processing Pipelines: Intelligent evidence prioritisation systems with configurable workflows that automatically identify, classify, and rank digital artefacts based on investigative relevance, incorporating AI-driven analysis capabilities and automated compliance verification.
- Lawful Access Solutions for Encrypted Data: Technical approaches for lawfully accessing encrypted communications whilst preserving user privacy and communication security through metadata analysis, cloud service integration, and legal compliance frameworks.
- Next-Generation Cryptographic Analysis Capabilities: Advanced decryption platforms addressing current technological limitations and quantum-resistant approaches, with scalable processing architectures and integration potential with Europol's infrastructure.

## 2. Intelligence Analysis and Multi-Modal Data Processing

**Context:**

Digital evidence is key in 85% of investigations, yet LEAs lack necessary technology and resources to effectively process vast data volumes. Solutions must address critical operational gaps whilst supporting Europol's digital transformation priorities.

**Innovation Areas:**

- Multi-modal Data Intelligence Processing: Real-time multi-source data fusion capabilities processing SIS alerts, CCTV, social media, and crypto flows with AI-powered pattern recognition and automated filtering systems. Mapping Internet criminal infrastructure: mapping & reconnaissance of C2 servers, DNS abuse, botnets …
- Advanced Digital Forensics Technologies: Quantum-resistant decryption platforms, cloud-native forensic frameworks, and IoT device data extraction capabilities with EU-compliant automated evidence processing. Software/initiatives to counter phishing/social engineering campaigns or spoofing.
- Intelligent Data Pre-processing: Universal data format harmonisation with automated classification and semantic mapping, implementing technology-neutral categorisation frameworks supporting cross-Member State compatibility.
- Cryptocurrency Investigation Solutions: Cross-chain blockchain analytics with real-time transaction monitoring and de-anonymisation techniques for mixers, tumblers, and DeFi platforms, providing comprehensive visualisation and automated asset recovery reporting.
- Financial Intelligence Sharing Platforms: Secure multi-institution data integration with privacy-preserving analytics capabilities and automated suspicious activity detection compatible with EFIPPP framework.
- AI-Powered Disinformation Detection: Multi-modal deepfake detection across video, audio, and image formats with real-time social media monitoring and automated disinformation campaign mapping.

**3. Situational Awareness and Quantum-Safe Technologies**

**Context:**

Criminal networks operate across complex digital and physical environments requiring comprehensive real-time intelligence platforms. The quantum threat necessitates immediate preparation for post-quantum cryptography migration.

**Innovation Areas:**

- Digital Twin Mapping Platforms: Comprehensive data integration from digital forensics networks, financial intelligence, and communications intercepts with real-time criminal network visualisation and AI-powered pattern recognition.
- Secure Next Generation Communications Channels: Lawful access solutions enabling court-authorised access to encrypted communications whilst preserving encryption integrity, with next-generation decryption capabilities and AI-enhanced data processing.
- VR/XR Training Solutions: Immersive scenario development for digital forensics investigations, cyber-crime scenes, and counter-terrorism operations with adaptive learning systems and cost-effective deployment.

- Post-Quantum Cryptography Implementation: Solutions based on NIST-approved quantum-resistant algorithms with transition management systems and threat detection capabilities identifying quantum-based attacks.
- 3D Printed Weapons Detection: Advanced detection technologies for identifying 3D-printed weapon components with AI-powered monitoring systems and forensic analysis capabilities for tracing manufacturing sources.

**4. Uncrewed Systems for Law Enforcement Operations**

**Context:**

Current operational gaps exist in surveillance capabilities, tactical response, threat mitigation, and force protection as criminal networks exploit advanced technologies for detection evasion.

**Innovation Areas:**

- Multi-Mission Operational Platforms: Surveillance, search & rescue, and Explosive Ordnance Disposal operations with autonomous capabilities, enhanced sensor integration, and real-time data transmission.
- Swarm Solutions: Coordinated multi-platform systems (3-100+ units) with synchronised operations, distributed intelligence, and autonomous coordination capabilities with adaptive mission execution.
- C-UAS Detection and Mitigation: Comprehensive counter-drone systems providing detection, identification, tracking, and neutralisation with multi-layered defence and selective mitigation capabilities.
- Unmanned Security Vehicles: Autonomous ground and maritime platforms for persistent surveillance and patrol with advanced navigation and multi-sensor integration capabilities.
- AI/Robot Convergence Solutions: Integrated AI-robotics platforms with advanced decision-making algorithms, predictive threat analysis, and autonomous response capabilities.

**5. Synthetic Content Detection and Authentication**

**Context:**

Criminal networks massively exploit generative AI to create hyper-realistic content facilitating fraud, child exploitation, and disinformation, necessitating innovative technological solutions for digital evidence integrity.

**Innovation Areas:**

- Automated Multi-Modal Detection: Real-time detection and large-scale processing capabilities for identifying synthetic content (video, audio, image) with integrated multi-modal approaches and continuous adaptation to new generation techniques.
- Content Authentication and Traceability: Robust and imperceptible watermarking with cryptographically secured provenance metadata, open standards compatibility (C2PA, W3C), and real-time integrity verification.

**Requirements:**

Detection rate >95%, false positives <2%, processing capacity >1,000 files/hour, explainable decisions for forensic context, and detailed reports usable in court proceedings.

**6. Sovereign Cloud Solutions and EU-Compliant Data Management**

Context:

Digitalisation of criminal activities requires secure access and analysis of sensitive data within EU jurisdiction whilst ensuring full regulatory compliance and protection against conflicting jurisdictional requirements.

Innovation Areas:

- AI-Enhanced Cybersecurity Solutions: Next-generation AI-powered security technologies protecting sensitive law enforcement data with automated vulnerability discovery, AI-driven forensics platforms, and behavioural analysis capabilities countering AI-enhanced criminal tactics.
- EU-Compliant Cross-Border Data Access Tools: Technical solutions streamlining cross-border digital evidence collection whilst maintaining judicial oversight, providing direct law enforcement-service provider frameworks with mechanisms detecting and blocking unauthorised foreign access requests.
- Sovereign Cloud Platforms with Built-in Compliance Framework: EU-based cloud platforms featuring comprehensive sovereignty controls and "lawful access by design" architecture with EU-wide data residency, automated compliance verification for GDPR/AI Act/Data Act, and advanced encryption with EU-controlled key management.

**7: Next-Generation Biometric Analysis Solutions**

Context:

European Law Enforcement Agencies (LEAs) are facing evolving challenges in biometric identification and verification, particularly in forensic contexts where traditional fingerprint analysis may be insufficient or unavailable. Two emerging biometric modalities - dorsal hand analysis and voice recognition - present significant opportunities to enhance investigative capabilities and forensic identification processes. LEAs require innovative solutions that can be seamlessly integrated into existing forensic workflows while maintaining compliance with European legal frameworks and fundamental rights protections.

Innovation Areas:

- Dorsal Hand Analysis:
  No forensic capabilities for analysing dorsal hand features when fingerprints are unavailable or compromised
  Need for automated systems that can process partial or degraded dorsal hand evidence
  Integration challenges with existing forensic databases and case management systems

  **Key Requirements:**

  Requirement for court-admissible evidence processing with full audit trails
  Innovative Solutions for Automated Dorsal Hand Analysis:
  Innovative solutions that harness AI models to automate the analysis and comparison of morphological features on the dorsum of the hand, skin features and other patterns of interest for the comparison, identification of individuals and verification of their identity in a forensic context
  High-resolution imaging analysis with enhanced feature extraction from partial or degraded samples
  Compatibility with existing forensic imaging standards and evidence chain requirements
  Database integration capabilities for cross-referencing with known subjects

- Voice Recognition:
  Need for robust voice identification systems that can operate with low-quality audio evidence and various sources.

Anti-spoofing capabilities to detect synthetic voice manipulation in criminal investigations
Multi-language processing for cross-border investigations
Real-time voice comparison for ongoing surveillance operations

**Key Requirements:**

Advanced Voice Technologies:
Forensic-grade voice biometric engines with neural network-based feature extraction
Robust detection of synthetic voice manipulation and deepfake audio evidence
Multi-modal voice analysis supporting various audio qualities and recording conditions
Integration with existing audio forensic workflows and evidence management systems

**Forensic Integration and Compliance:**

EU legal framework compliance with admissible evidence standards
Integration with existing LEA forensic infrastructure and audit trails and chain of custody documentation
Privacy protection measures in accordance with fundamental rights requirements
Evaluation Criteria
Presentations will be assessed on forensic accuracy and reliability, legal admissibility standards, integration with LEA systems, operational scalability, cost-effectiveness for public procurement, evidence integrity preservation, and demonstrated law enforcement validation.

## General compliance requirements:

GDPR, AI Act, Data Act, NIS2 Directive compliance with demonstrated operational independence from non-EU jurisdictions and legal frameworks.