SHIELD PCP

Open Market Consultation Document

Open Market Consultation for the future Pre-Commercial Procurement of R&D services in the field of protection of public spaces and crowd management

December 2025

Funded by the European Union

Disclaimer and copyright

This document (including the accompanying annexes) has been drafted with the utmost care, but no guarantees are given regarding its soundness and/or completeness. Any errors or inaccuracies can be reported via email to email contact@shieldpcp.eu.

The SHIELD PCP consortium is not responsible for the correct operation of any URL mentioned in this document, nor for the proper functioning of any electronic platform used (for example, the EU survey system). Any problems encountered when using a URL and/or an electronic platform must be reported to the organisation that makes the URL or the electronic platform available. Problems with downloading and uploading (of documents) must also be reported via email to contact@shieldpcp.eu.

Economic operators and other stakeholders are being informed that any information regarding the setup and execution of both the procurement process and the execution of any contract/framework agreement as a result of the procurement process as well as public summaries of the results of the PCP project, including information about key R&D results attained and lessons learnt by the procurers during the PCP, can be shared after consultation with the respective R&D provider by the SHIELD PCP consortium with(in) the context of the contract and consequently can be analysed, (re-)used and published by the SHIELD PCP consortium. Details should not be disclosed that would hinder the application of the law, would be contrary to the public interest, would harm the legitimate business interests of the R&D providers involved in the PCP or could distort fair competition between the participating R&D providers or others on the market.

The SHIELD PCP receives funding under the European Union's Horizon Europe framework program for research and innovation under the grant agreement No 101225962. The EU is, however, not participating as a contracting authority in the procurement.

A Prior Information Notice, or PIN, has been published in TED on 24.11.2025 to announce the Open Market Consultation on potential future procurement activity (notice publication number: 784497-2025 - Planning - TED).

The original language of this open market consultation is English.

Abbreviations and acronyms

CET	Central European Time
COTS	Commercial Off-The-Shelf
EAFIP	European Assistance for Innovation Procurement
EC	European Commission
EU	European Union
FAIR	Findable, Accessible, Interoperable and Reusable
FRAND	Fair, Reasonable and Non-Discriminatory
GDPR	General Data Protection Regulation
GPA	Government Procurement Agreement
HE	Horizon Europe
IPRs	Intellectual Property Rights
OMC	Open Market Consultation
PBG	Public Buyers Group
PCP	Pre-Commercial Procurement
PIN	Prior Information Notice
R&D	Research and Development
RFI	Request For Information
SMEs	Small and Medium Enterprises
SOTA	State Of the Art
TED	Tenders Electronic Daily
TRL	Technology Readiness Level

Funded by the European Union

Key definitions

Consortium	Group of public and/or private entities (including public buyers and supporting organisations) that are part of the SHIELD PCP. For more information: https://shieldpcp.eu/
Contractor	A company or entity that has been awarded a contract under the PCP.
Lead Procurer	A Public Buyer who acts as a Procurer in the PCP and purchases the R&D services on behalf of itself and other Public Buyers (in this case, FMI).
Public Buyer	A public entity that purchases goods or services from the market and is subject to the public procurement regulation.
Technology Provider	A company or entity that develops and/or sells technology in the market.

Contents

1. Purpose of the Open Market Consultation

1.1. Scope and main objectives

This document outlines the objectives and procedures of the Open Market Consultation (OMC) for the SHIELD PCP project – a forthcoming Pre-Commercial Procurement (PCP) in the field of protection of public spaces and crowd management.

The OMC formally commences with the publication of a Prior Information Notice (PIN) in the Tenders Electronic Daily (TED) and concludes on the date indicated in this document, unless terminated earlier by the public buyers. Through this OMC, the SHIELD PCP Public Buyers Group (PBG) – led by the French Ministry of Interior – aims to challenge the market to provide input and insights on innovative solutions addressing critical security scenarios in public spaces (see Section 2.5), by improving multi-agency coordination, situational awareness, and crowd safety.

In this context, the OMC serves to inform technology providers, research institutions, end-users (e.g. security practitioners), and other stakeholders about the needs and requirements of the buyers, and to gather their feedback on the SHIELD PCP challenge. Another key objective is to assess the market's capability to meet these needs and to obtain input on the feasibility of the procurement plans and conditions described in this document (and its annexes). In sum, the OMC seeks to:

1. Validate the state-of-the-art analysis findings and the viability of the preliminary technical and financial assumptions
2. Raise industry awareness about the upcoming PCP and its opportunities
3. Collect insights from the market to fine-tune the PCP tender specifications.

This OMC is conducted under the law of the Lead Procurer (French law).

The contracting authorities involved are not legally bound by any outcome of the OMC. Launching this OMC does not obligate the buyers to initiate a procurement; if a PCP call is subsequently launched, the PBG reserves the right to adjust or refine any element of the challenge and requirements based on OMC feedback. Participation in the OMC is voluntary, open, and non-binding. The OMC is not part of any pre-qualification or selection process, and no advantage or disadvantage will be given to any supplier or group of suppliers as a result of participation.

All information shared during the OMC (excluding any confidential solutions details) will be published openly in English on the project website, ensuring transparency and equal treatment of all parties.

Where appropriate, parts of the information received from market parties can be shared with the EC.

1.2. Who can participate?

The OMC is open to all interested parties – in particular to technology providers (companies including start-ups, SMEs, large industry, etc.) and end-users such as public authorities, first responders, law enforcement agencies, and security operators. However, please note that only suppliers eligible for Horizon Europe PCP actions (i.e. established in EU Member States or Associated Countries and committing to perform the R&D services within those countries) will be eligible to participate in the subsequent PCP procurement.

Participation in the OMC is voluntary and non-binding and is at the own expense and risk of market operators. A market operator cannot charge any costs to the PBG for participation in the OMC or for (re-)use of its information in the context of a future procurement procedure.

Participation in this OMC is not a condition for submitting a tender in the subsequent procurement, does not lead to any rights or privileges for the participants, and is not part of any pre-qualification or selection process. The provided input in this OMC will not be used to evaluate future proposals.

1.3. Activities & timetable

The SHIELD PCP Open Market Consultation will be carried out through a combination of events and interactions designed to promote a two-way dialogue with the market.

- A main (hybrid) event in Paris (France) in February 2026. This event will be carried out in English and broadcasted online.
- A series of webinars in different EU languages will be held from 27 to 29 January 2026.
- A Request for Information (RFI) questionnaire using the EU Survey tool: https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire

- Other activities as deemed necessary within the scope of the project.

The timetable of activities and required actions of the OMC is as follows:

Date	Event
24 November 2025	Publication of the Prior Information Notice (PIN) on TED.
18 December 2025	Publication of the OMC documents on the project's website: www.shieldpcp.eu Publication of the EU Survey questionnaire: https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire
27 January 2026	OMC webinar in French
27 January 2026	OMC webinar in Spanish
28 January 2026	OMC webinar in Slovak
29 January 2026	OMC webinar in Polish
29 January 2026	OMC webinar in Italian
24-26 February 2026	OMC event in English - Paris, France (hybrid) [9:00-15:00 CET
6 March 2026	Deadline for the submission of answers to the questionnaire in the EU Survey (17:00 CET)
12 March 2026	Publication of the OMC report
13 March 2026	Closure of the OMC

The SHIELD PCP consortium is entitled to adjust the planned activities and the timetable above, and to include new activities at any time according to the needs and responses of the market. Furthermore, it may decide to terminate the OMC for its own reasons at any time. In that case, the SHIELD PCP consortium will publish such modifications or termination on TED and the project's website (https://shieldpcp.eu/).

The events and webinars celebrated within the framework of the OMC will be recorded. In that case, by attending the physical event, you will consent to be

recorded. By using your video and microphone during the webinars, you will consent to be recorded. If you do not want your voice and image to be recorded during the webinars, you may ask your questions using the chat. The SHIELD PCP consortium shall use those records for the purpose of the project only.

In addition, please be aware that photos may be taken during the meetings. The SHIELD PCP consortium shall use those photos for the project only.

1.4. Registration

Registration is required to participate in the OMC webinars and the hybrid event in Paris. Interested participants are asked to register via the online form available on the SHIELD PCP website: https://shieldpcp.eu/tender/#:~:text=Register%20for%20the%20Open%20Market%20Consultations

Registration is free of charge. In the registration form, you will be asked to provide basic information (name, organisation, contact details, etc.) and indicate which session(s) you plan to attend (webinar language and/or the Paris event). Early registration is encouraged, as it will help the organisers in planning the sessions and logistics.

For the hybrid event in Paris, on-site attendance may be limited by venue capacity, so prior registration is essential (places will be confirmed by the organisers). Due to capacity constraints, priority for on-site participation may be given to organisations that have submitted a completed RFI questionnaire. Online participants will receive webinar access details by email after registration. The project will ensure that remote attendees can fully engage with the event (live streaming of presentations and an interactive Q&A/chat for questions).

Please note that by registering, participants agree to the project's privacy policy regarding the handling of personal data. Personal data will be used solely for the purposes of organising the OMC and will be treated as confidential in compliance with GDPR (EU Regulation 2016/679).

1.5. Procedure

The OMC starts on the date of its publication in TED and ends on the date set in the timetable, unless terminated earlier.

Interested parties are requested to register through the link provided above in order to participate in the events and receive additional information about the project. The questionnaire should be filled out before the deadline indicated in the timetable above.

The SHIELD PCP consortium will support interested parties throughout the whole OMC during the events and by answering questions through a Q&A document, which will be published on the project's website.

Additional written contributions in the form of a Request for Information (RFI) questionnaire or other questionnaires (via the EU Survey platform), aiming to collect market information on innovative and commercial solutions, may be requested.

The responses to the questionnaires should not contain any confidential information. As the questionnaire is intended to explore the market "as is", there are no right or wrong answers. The answers provided will be used as input for the procurement strategy and contract conditions.

After processing and analysing the answers, the SHIELD PCP consortium will disseminate the results to the widest possible audience. Nevertheless, all answers provided by market parties will be anonymised and treated as confidential. The SHIELD PCP consortium will therefore not provide information about specific answers from market operators. Only the general findings and a summary of the answers will be provided. The results of this OMC will be published on the project's website.

In case the information provided in this document and annexes needs further clarification, market operators may ask questions during the events, or via the contact email address (contact@shieldpcp.eu).

Market operators who wish to provide additional confidential information during the OMC can send an email to the email address indicated above. The information must be clearly marked as confidential. Confidential information will not be included in the OMC report.

1.6. Annexes

The following annexes are part of this document:

- Annex I – Request for Information questionnaire.

- Annex II – Use cases.
- Annex III – Requirements.

The annexes form an integral and inseparable part of this OMC document. In the event of any conflict between the provisions of this document and the annexes, the provisions of the OMC document shall prevail.

2. SHIELD PCP Scope

2.1. Context and objectives

SHIELD PCP (Security Harmonised Innovation for Enhanced Law Enforcement Capacities in Dynamic Crowd Protection) is a European Union-funded project that brings together first responders, public authorities, and technology providers to co-create innovative solutions for protecting public spaces. The project addresses the growing challenge of keeping public venues and urban spaces safe amid evolving security threats – from terrorism and organised attacks to incidents of crowd panic and unrest. Developing effective solutions that meet diverse operational needs across different countries and domains remains difficult, as many off-the-shelf products are inadequate or fragmented. SHIELD PCP seeks to overcome this gap by actively involving the "demand side" (security buyers and end-users) in defining their unmet needs and steering industry R&D efforts towards those needs.

Building on the groundwork of its predecessor project SHIELD4CROWD, which identified common vulnerabilities and technology gaps in public space security, SHIELD PCP now moves from problem analysis to action, turning the shared needs into concrete innovation procurements. The core objective of SHIELD PCP is to drive innovation through a Pre-Commercial Procurement, empowering a group of public buyers to jointly stimulate the development of cost-effective, cutting-edge security solutions tailored to their real-world requirements. In particular, the project aims to deliver new tools that enable seamless coordination and cooperation among all stakeholders (especially law enforcement agencies) during major security incidents, thereby enhancing the overall safety and resilience of public spaces.

The infographic below illustrates a simplified conceptual flow of how an integrated crowd-management solution could function within the context of the SHIELD PCP challenge areas.

Figure 1: Conceptual flow of SHIELD PCP[1]

In summary, SHIELD PCP's vision is to produce scalable and interoperable solutions that improve situational awareness, multi-agency response coordination, and smart crowd management in dynamic environments where large crowds are present. By the end of the project, the goal is to have validated prototypes that can be readily adopted by security practitioners across Europe – filling current capability gaps and leveraging modern technologies (such as artificial intelligence, sensors, secure communications, etc.) for safer public spaces.

2.2. PCP challenge and main requirements

The envisaged future PCP – i.e. a joint procurement of R&D services – is intended to be launched to reinforce public demand-driven innovation in the security domain. PCP has the potential to be an effective demand-side innovation action and a useful tool to close the gap between supply and demand for innovative solutions. Solutions are expected to achieve TRL 7-8.

The future PCP should deliver successful, innovative and fully tested product(s) and/or service(s) that meet the common need of the PBG to procure research, develop

[1] It is provided solely for explanatory purposes and does not represent the final or complete workflow of the intended solution. The actual processes, technical architecture and operational steps may evolve or differ as the project progresses and as inputs from the market and end-users are assessed.

innovative marketable solutions, speed up the time-to-market and provide best value for money.

The PBG aims to develop an innovative solution to tackle the use cases concerning Panic at football stadium (Slovakia), Drone Attack Match Day (Spain), and Multi-actors coordination after a massive knife attack in a train station (France).

For each use case, the innovative solution is expected to cover the different steps and functionalities as described in Annex II and Annex III.

2.3. The Pre-Commercial Procurement approach

This OMC concerns a future PCP of R&D services to be performed in their majority in the EU Member States or Associated Countries.

PCP is an approach that allows public procurers to buy R&D from several competing technology providers in parallel, to compare alternative solution approaches, and to identify the best value-for-money solutions that the market can deliver to address their needs. In PCP, there is a risk-benefit sharing under market conditions between the public procurer and the technology providers, and a clear separation between the PCP and the deployment of commercial volumes of end-products.

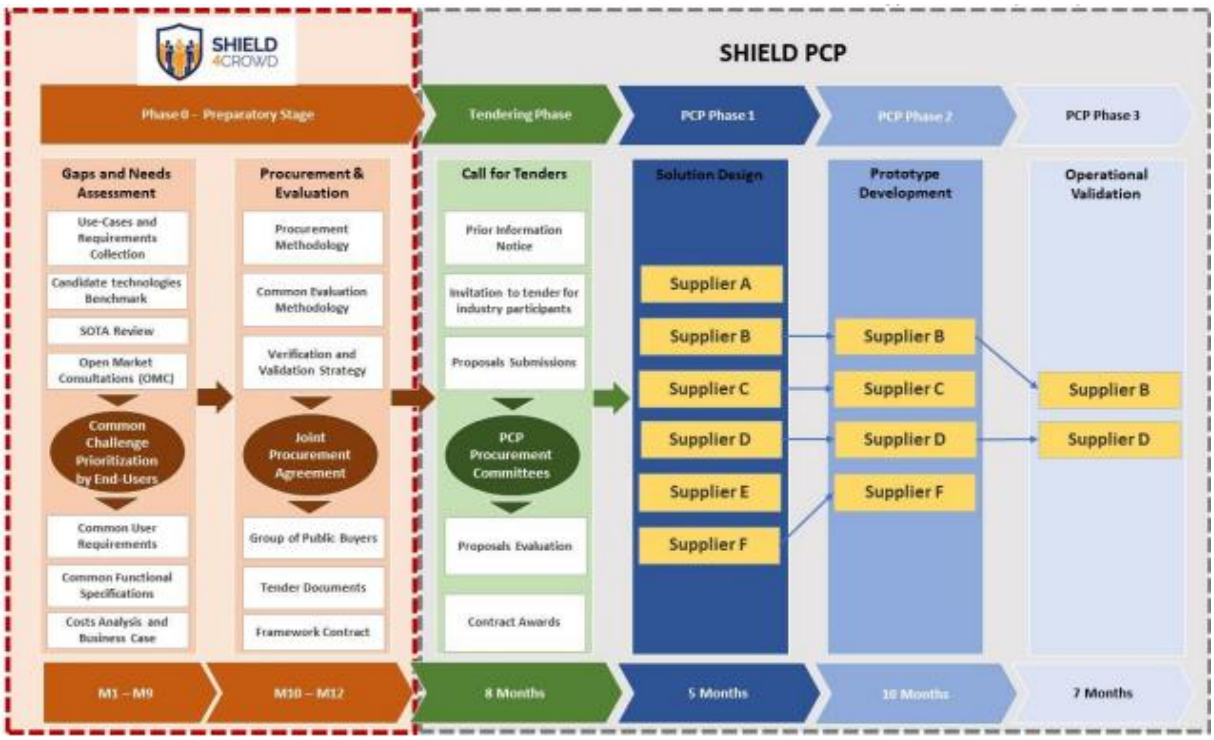

Figure 2: SHIELD PCP Innovation Procurement Phases.

Along with the R&D services, the PCP allows to purchase of some products provided that the value thereof is **less than 50 % of the total value of the contract**.

The PCP tender will start with the publication of the contract notice along with the request for tenders, the framework agreement, and the phase contracts. After evaluating the offers submitted by the technology providers according to the rules established in the tender documents, the contracts will be awarded, and a contract award notice will be published. The process will be monitored to ensure sound deployment, integration and validation of the PCP.

The PCP procedure is composed of three phases: solution design, prototype implementation, and validation and demonstration of the solutions.

Phase 1. Solution design: During this phase, the contractors will be asked to describe the solution, providing the complete architecture and design thereof and verifying the technical, economic and organisational feasibility of their solution to address the PCP challenge.

Phase 2. Prototype implementation: This phase concerns the development of the first prototypes of the solutions, which will be tested. Contractors will develop a first prototype based on the design documents delivered in the previous phase and test their solutions in lab conditions. Prototypes will be tested and verified to provide a measure of the technical performance of each solution in a controlled environment. During and at the end of phase 2, the PBG will request from the contractors a series of deliverables in order to evaluate their progress and the performed activities and the obtained results.

Phase 3. Validation and demonstration of the solutions: It will validate the final solutions (at least two) in diverse conditions, using the detailed scenarios and processes developed in the verification and validation strategy. During phase 3, a feedback mechanism will be established between the PBG and the selected contractors in order for the latter to receive requests for improvements directly from the end users. The Public Buyers will request from the contractors an Integration Report. Finally, a Field Acceptance Report related to the accomplishment that the two final solutions, which have been deployed and that the validation tests have been successfully performed in a real operational environment, will be requested.

After each phase, intermediate evaluations will be carried out to progressively select the best of the competing solutions. The contractors with the best-value-for-money solutions will be offered a specific contract for the next phase.

The contractors will retain ownership of the IPRs that they generate during the PCP and will be able to use them to exploit the full market potential of the developed solutions.

Contracts implementation

During the implementation of the SHIELD PCP, effective tools will be used in order to monitor the performance of the R&D suppliers and provide regular feedback during each phase. Each contractor will be assigned a main contact person (their supervisor) appointed by the procurers as the main point of contact.

More specifically, the monitoring process will be divided into 3 sets of activities:

- **Pre-monitoring**: A kick-off meeting per contractor will be scheduled at the beginning of each PCP phase, and the selected contractors will be requested to present their implementation schedule for the PCP phase that they are entering. During the same meeting, the supervisor will present the framework for the review. The objective is to establish a close and fruitful communication channel with the contractors, in order to ensure from the early beginning of the action that the project is implemented according to the needs of the buyers.
- **Monitoring**: Contract implementation will be monitored and reviewed against the expected outcomes for each phase. The intensity of monitoring and communication between the PBG and the contractors will increase from phase 1 to phase 3. For instance, regular meetings with the contractors by video call or face-to-face, on-site visits to the contractors' locations to check and discuss the status of the work and progress, or any other suitable way. Ad-hoc meetings and on-site inspections are also possible in the event that the R&D development has halted or slowed down.

  The contractors are mandated to present monthly the current status of the work and describe the progress made. All the documentation generated by the contractors will be reviewed, and the ideas and recommended areas to pursue will be highlighted in post-review activities.

- **Post-monitoring**: At the conclusion of the monitoring activities, the supervisor will provide written feedback for each contractor at each PCP phase. This feedback will generally consist of overall comments and remarks about the contractor's outcomes under review. Monitoring activities will be continued after the PCP is completed. Specifically, it will be checked whether the contractors are successfully commercialising the R&D results within the call-back period defined in the PCP framework agreement. If that is not the case, the SHIELD PCP consortium will ask the R&D suppliers to give licenses under FRAND terms to other third parties or to transfer back the ownership of results to the PBG.

2.4. The Public Buyers Group

The SHIELD PCP consortium's Public Buyers Group (PBG) consists of four public buyers from three EU Member States (France, Spain, and Slovakia). The PBG includes the Ministries of Interior of France, Spain, and Slovakia, as well as France's national railway company (SNCF). For the purpose of the PCP, the PBG is represented by the French Ministry of Interior as the lead procurer, acting on behalf of all buyers.

Ministère de l'Intérieur et des Outre-mer (France) – The French Ministry of the Interior ensures the safety and security of the French population and addresses its security concerns and public service needs. It plays a central role in law enforcement, crisis management, and immigration matters. The Ministry oversees the National Police and Gendarmerie, ensuring these law enforcement agencies can carry out their missions to safeguard people and property while respecting citizens' rights and liberties. A crucial objective of the Ministry is to protect citizens from emerging threats by leveraging specialised intelligence services in the fight against organised crime and terrorism. Additionally, the Ministry manages responses to crises (technological accidents, natural disasters, terrorist attacks, etc.), working to protect and assist the population through agencies like Civil Security and the national firefighters. The Ministry is also responsible for coordinating between central and local government authorities and handling issues related to both legal and illegal immigration.

Ministerio del Interior (Spain) – The Spanish Ministry of the Interior oversees public security and the protection of constitutional rights in Spain. Its responsibilities include law enforcement, national security, immigration and border control, prison

administration, civil defence, and road traffic safety. The Ministry manages a substantial budget (approximately €24.6 billion annually, ~2.1% of Spain's GDP) to fulfill its mission. Key agencies under the Spanish Ministry of Interior include the Civil Guard, the National Police Corps, the Intelligence Center for Counter-Terrorism, the State Security Infrastructure and Equipment Office, and the prison administration agency. The Spanish National Police (established in 1824, with over 64,000 officers) exemplifies the Ministry's focus on modern, technology-supported approaches to enhance public security and safety.

Ministerstvo vnútra Slovenskej republiky (Slovakia) – The Ministry of Interior of the Slovak Republic is the central state authority for internal affairs, including public order, the security of persons and property, protection and administration of state borders, immigration and the stay of foreigners, as well as issuance of national identity documents (IDs, passports, driver's licenses). It oversees the Police Force and the Firefighting and Rescue Corps, among other agencies.
The Ministry's Department of Public Procurement is responsible for procuring goods, services, and works for the Ministry's needs, ensuring that public contracts are completed on time, within budget, and to specification. The Ministry of Interior of the Slovak Republic has extensive experience in procuring security solutions financed by the state budget or EU funds – for example, procurement of firefighting vehicles, flood protection equipment, and various personal equipment for police forces.

Société Nationale des Chemins de fer Français (SNCF) – France – SNCF is France's national state-owned railway company, responsible for passenger and freight rail services and the management of railway infrastructure, including major hubs like Paris's Gare du Nord. As a public transport operator, SNCF plays a vital role in ensuring security across its network of stations and trains. It maintains its own railway security service ("Sûreté ferroviaire") with officers dedicated to protecting passengers, staff, and infrastructure from crime and safety threats. SNCF works in close collaboration with the French Police and Gendarmerie, especially via the Prefecture of Police in Paris and other regional authorities, to prevent and respond to incidents such as vandalism, violence, or terrorist threats in train stations and on trains. By participating in SHIELD PCP, SNCF brings valuable expertise in securing crowded transport environments and

will help shape innovative solutions to enhance the security and resilience of public spaces in transit hubs.

3. Market analysis: preliminary results

This section presents the preliminary results of the market analysis, which aims to identify existing technologies that can tackle the procurement challenge and to estimate the TRL thereof. It started with the publication of a Call for Information to gather information from potential technology vendors about their products, services, and capabilities.

Preliminary analysis of the patent landscape indicates that several technological building blocks relevant to SHIELD PCP, such as AI-based crowd monitoring, multi-sensor data fusion, geolocation and tracking, and drone/anti-drone capabilities, are well represented in existing innovations. These patents demonstrate a strong maturity in analytics, sensing, and situational awareness components. However, the analysis also highlights significant gaps in areas essential for the integrated, multi-agency nature of SHIELD, namely, shared and role-based Common Operational Pictures, command hierarchy and workflow management across multiple authorities, coordinated decision-making tools, public information and alerting mechanisms, interoperability and architecture-level integration, and most non-functional requirements (e.g., usability, privacy-by-design, governance, and deployment models). **No single patent or existing solution covers the full range of SHIELD PCP requirements**, confirming the need for innovation procurement to stimulate development of holistic, interoperable, and cross-agency security solutions.

4. Request for information questionnaire

As part of the OMC, the SHIELD PCP consortium is seeking written feedback from technology providers, system integrators, research institutions, and all relevant stakeholders via a Request for Information (RFI) questionnaire. The RFI is available online via the EU Survey tool [https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire], and the questions are also listed below for reference.

Please note that taking part in this survey is not a prerequisite for participation in the future PCP and does not give any advantage to any technology provider. SHIELD PCP

will ensure transparency, openness, and equal treatment of all economic operators. All information provided in the questionnaire will be anonymised, summarised and published online in English on the project's website.

Your personal data will be collected, processed, stored and used by the SHIELD PCP consortium with the sole purpose of gathering information from the market within the framework of the SHIELD PCP. Personal data will be treated as strictly confidential according to the General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council - GDPR). You may exercise your right to access your personal data and the right to rectify such data by contacting: contact@shieldpcp.eu.

Annex I Request for Information questionnaire

GENERAL INFORMATION	
Name of your organisation: **Website:** **Email address:** **Type of organisation:** • ☐ **Start-up** • ☐ **SME** • **Large company** • ☐ **Public organisation** • ☐ **Private organisation** • ☐ **R&D institute / University** • ☐ **Other:** _____ **Country:** **Contact person name & email:**	
PCP challenge and requirements	
1.	Are you aware of any existing or emerging technologies in the field of protection of public spaces and crowd management (as described in SHIELD PCP)? YES/NO Please elaborate.
2.	Are you currently developing or have you developed any solution relevant to any of the following use cases? *(Tick all that apply and describe briefly)* • ☐ Use Case 1: Panic at football stadium. • ☐ Use Case 2: Drone Attack Match Day. • ☐ Use Case 3: Multi-actors coordination after a massive knife attack in a train station. • ☐ No solution was developed for any of the use cases above. Please explain your solution (or concept) and its key functionalities.
3.	Which of the following capability areas do you consider **most critical** to address these scenarios? *(Select up to 3 options.)* • Real-time common operational picture (COP) and dashboards for commanders • Crowd behaviour monitoring and analytics (e.g. detecting surges, panic) • Counter-drone detection and neutralisation systems • AI-supported decision-making tools for incident management • Inter-agency communication and coordination platform • Multi-source data fusion and sensor integration • Evacuation support and crowd routing systems • Public alerting and communication to citizens (e.g. emergency messaging)
4.	What are the safety mechanisms and fail-safe features your solution would include to avoid collateral damage or unintended consequences?
5.	Do you identify any technical, operational or organisational barriers, gaps or missing needs in relation to the scope and requirements of SHIELD PCP? YES/NO Please explain.
6.	Can your solution be modularised or integrated with external platforms or APIs (e.g., EMS, law enforcement systems)? *(Yes/No)* If yes, please specify:

7.	If you were to participate in the SHIELD SHIELD PCP, please indicate your indicative time allocation (in months) for each of the following phases: (Total should not exceed 23 months.) • Phase 1: Solution Design (months): _____ • Phase 2: Prototype Development (months): _____ • Phase 3: Validation & Demonstration (months): _____ • Please briefly justify your estimated time:
8.	If you were to participate in the SHIELD PCP, please provide your indicative budget allocation (in EUR) per PCP phase: *Note: Please be aware that there is a predefined budget allocation for this PCP project, and the total available budget will be divided across phases and participating contractors. For the purpose of this question, please assume a total indicative PCP budget of* ***EUR 3,500,000****.* • Phase 1: Solution Design (€): _____ • Phase 2: Prototype Development (€): _____ • Phase 3: Validation & Demonstration (€): _____ • Please briefly justify your estimated budget distribution:
9.	Do you feel that the use cases and requirements described (spanning common operational picture, crowd monitoring, geolocation tracking, communications, etc.) cover all the critical needs of the PCP challenge? Are there any significant challenges or needs that you believe are missing from our list?
10.	Which of the listed requirements in Annex III do you anticipate being the most technically or operationally challenging to implement, and what makes them challenging? Please highlight any requirements you see as high-risk or particularly complex.
11.	What do you anticipate will be the **main cost drivers** in developing and deploying an integrated solution for these scenarios? *(Select up to 2 options.)* • Specialised hardware (e.g. sensors, drones, cameras) • Software development (analytics, AI algorithms, user interfaces) • System integration of components and data sources • Communication infrastructure (networks, devices, radios) • Training and change management for end-users • Ongoing maintenance and support of the system. • Other
12.	Which approach do you believe is more effective for delivering the solution sought in this PCP? *(Select one option.)* • A single-vendor integrated platform (one provider/consortium delivering all components as a unified system) • A modular solution (multiple specialised components from different providers, designed to interoperate) • No strong preference / Either approach can work
13.	How important is it that the solution uses open standards and interfaces to interoperate with existing systems and third-party components? *(Likert scale: 1 = Not important, 5 = Very important)*
14.	Can you provide any other recommendations regarding the SHIELD PCP solution(s)? YES/NO Please elaborate if any.
State-of-the-art analysis	
15.	Do you think there is room for technological development beyond the state of the art? YES/NO Please explain.

16.	What is the current Technology Readiness Level (TRL) of your solution(s) or their main components? *Please indicate the TRL for the relevant functional requirement groups described in the OMC document (Annex III), if applicable.*
17.	What are the main limitations of the current state of the art that your solution aims to address, and what improvements would it introduce compared to existing approaches?
18.	Do you rely on any patented technology or standards? • ☐ Yes • ☐ No • ☐ Please list relevant patents or standards.
19.	Are there existing patents or intellectual property barriers that could limit your solution's development or deployment? YES/NO Please explain.
20.	Which of the following areas already have mature solutions available on the market (high readiness, e.g. TRL 8–9)? (*Select all that apply*.) • Real-time common operational picture (COP) and dashboards for commanders • Crowd behaviour monitoring and analytics (e.g. detecting surges, panic) • Counter-drone detection and neutralisation systems • AI-supported decision-making tools for incident management • Inter-agency communication and coordination platform • Multi-source data fusion and sensor integration • Evacuation support and crowd routing systems • Public alerting and communication to citizens (e.g. emergency messaging) • I do not know.
21.	In which areas do you see the least mature state-of-the-art, requiring the most innovation? (*Select up to 3 options that represent the biggest gaps*.) • Real-time common operational picture (COP) and dashboards for commanders • Crowd behaviour monitoring and analytics (e.g. detecting surges, panic) • Counter-drone detection and neutralisation systems • AI-supported decision-making tools for incident management • Inter-agency communication and coordination platform • Multi-source data fusion and sensor integration • Evacuation support and crowd routing systems • Public alerting and communication to citizens (e.g. emergency messaging) • I do not know.
22.	Which emerging technologies do you think could significantly enhance solutions for these scenarios? *(Select up to 3 options.)* • Artificial Intelligence / Machine Learning • Internet of Things (IoT) sensors and smart cameras • 5G or advanced wireless communication networks • Cloud computing and edge processing for real-time data • Advanced drone technologies and robotics • Big data analytics and predictive modelling • **Other:** *[please specify if applicable]*
Miscellaneous	
23.	What information do you still need to make a good plan of action for the development and/or implementation of solutions suitable to address the challenge?
24.	What additional information, requirements or conditions would you need to plan the development or deployment of a solution within SHIELD PCP? YES/NO If yes, please indicate them below:

25.	Would your organisation consider participating in the upcoming SHIELD PCP procurement (tender) as a solution provider? (Select one.) • Yes – we would likely participate • Maybe – we need more information/depends on conditions • No – unlikely to participate
26.	Do you intend to participate as a single entity or as part of a consortium? • Single entity • Consortium If participating as a consortium, please list the names of all consortium members: *(If not yet defined, indicate the complementary technologies or partners you are seeking.)*
27.	Could you please indicate the name of your proposed solution or innovation?
28.	Could you please provide an image or visual representation of your proposed solution or innovation, if available?
29.	Which modules or macro-functionalities does your proposed solution intend to address? • Real-time common operational picture (COP) and dashboards for commanders • Crowd behaviour monitoring and analytics (e.g. detecting surges, panic) • Counter-drone detection and neutralisation systems • AI-supported decision-making tools for incident management • Inter-agency communication and coordination platform • Multi-source data fusion and sensor integration • Evacuation support and crowd routing systems • Public alerting and communication to citizens (e.g. emergency messaging)
30.	How would you describe your technology, and how does it relate to the SHIELD PCP requirements?
31.	How would you describe the innovation level of your technology and its differentiation from the current state of the art? *(Please describe the innovation aspects of your solution, the state of the art in the market, and how your solution is differentiated.)*
32.	What is the target market addressed, and who will use your technology? *(Please indicate which user groups your solution addresses.)* • *Public bodies (e.g., law enforcement agencies, civil protection authorities, cities, defence sector)* • *Private-sector security operators (e.g., guarding services, event security management)* • *Mixed public-private security operators (e.g., critical infrastructure operators, utilities)* *Please provide additional details if needed.*
33.	What are the main technological, legal, ethical or operational risks and challenges associated with the development and deployment of your solution, and how could these be mitigated? *Please explain*.
34.	How do you consider the interoperability of the solution? *Please describe how your solution addresses interoperability with existing systems, standards, platforms, or infrastructure.*
35.	Did you already take part in a European project, or has the development of your solution /technology been co-funded by the European Union? *If so, please provide the name of the project, the Grant Agreement number and some further information.*
36.	How did you hear about the project SHIELD PCP?
37.	Do you have any suggestions and/or remarks?

Annex II – Use cases

Use Case 1: Panic situation in a football stadium
This use case addresses the management of a sudden panic situation during a high-attendance football match in a large urban stadium. The event is classified as high risk due to the presence of rival supporter groups and the concentration of spectators arriving through shared transport hubs and city-centre areas. Multiple public and private actors are involved, including public security authorities, emergency responders, and stadium security services, all operating under a unified but distributed command structure. During the match, a disruptive incident occurs within a crowded spectator area, leading to smoke, reduced visibility, and perceived danger. The situation escalates rapidly as fear spreads beyond the initial location, affecting nearby sections of the stadium. Crowd density increases in corridors and exit routes, complicating movement and evacuation. The combination of stress, noise, and limited situational awareness challenges both spectators and responders. Authorities must simultaneously manage public order, ensure life safety, and coordinate emergency response actions. This requires timely detection of suspicious behaviours or hazardous actions, continuous monitoring of crowd dynamics, and a clear understanding of how the situation is evolving across different areas of the venue. Effective intervention depends on real-time information sharing and coordinated decision-making among police units, fire and rescue services, medical responders, and private security staff. The use case highlights the need for integrated solutions that improve situational awareness, support multi-agency coordination, enhance communication with the crowd, and assist commanders in managing fast-evolving panic scenarios in complex, crowded environments.
Use case 2: Drone threat during a football match
This use case addresses the management of an emerging aerial threat during a major football match hosted in a large metropolitan stadium located in a dense urban environment with critical transport and infrastructure interconnections. The event involves high attendance and requires the coordinated presence of national police, emergency services, transport operators, and private venue stakeholders operating under established security protocols. During the match, an abnormal situation is detected involving multiple unmanned aerial systems (UAS) approaching the stadium airspace. The presence of drones in close proximity to a crowded venue triggers immediate security concerns and precautionary measures, including the temporary suspension of the event. The situation escalates as spectators become aware of the threat, leading to anxiety and the risk of uncontrolled crowd movements toward stadium exits and nearby transport facilities.

Authorities must manage the incident under significant time pressure, balancing the neutralisation of the aerial threat with the prevention of panic-induced crowd surges. Effective response requires rapid detection and tracking of UAS, resilient communications, and coordinated decision-making across law enforcement, emergency medical services, civil protection, and transport operators. Maintaining situational awareness both inside the stadium and in surrounding public spaces is critical to avoid secondary incidents. The use case highlights the need for integrated solutions combining advanced counter-UAS capabilities, real-time crowd monitoring, and secure multi-agency communication platforms. Such solutions should support commanders in managing complex, fast-evolving threats while enabling clear, timely communication with the public to reduce uncertainty and ensure safety in large-scale urban events.
Use Case 3: Multi-agency coordination following a violent incident in a major train station
This use case focuses on the management of a large-scale security incident occurring at a major international railway station with extremely high passenger volumes and complex interconnections between national, regional, and cross-border transport networks. The station operates as a critical mobility hub, welcoming hundreds of thousands of passengers daily and involving a wide range of public security authorities, emergency responders, transport operators, and private security services. The scenario considers the occurrence of simultaneous violent incidents within the station and in its immediate surroundings, leading to confusion, fear, and severe disruption of passenger flows. The rapid spread of uncertainty, combined with the high density of travellers, creates significant risks of panic, uncontrolled crowd movements, and secondary safety incidents. Multiple response units are required to intervene in parallel, while maintaining situational awareness across both indoor and outdoor areas. Effective crisis management in this context depends on the ability to quickly collect, fuse, and share information from heterogeneous sources in order to build a common understanding of the situation. Authorities must coordinate interventions, manage evacuations, and communicate clearly with passengers and staff, while tracking the deployment of responders and the evolution of crowd behaviour in real time. Delays or information gaps can significantly affect response effectiveness and public safety. The use case highlights the need for integrated solutions that enhance multi-agency coordination through a shared operational picture, support intelligent crowd management and evacuation guidance, and enable secure, real-time communication among all actors involved. Such capabilities are essential to reduce uncertainty, accelerate decision-making, and improve the overall management of complex security incidents in major transport hubs.

Funded by the European Union

Annex III – Requirements

1. Common operational picture & dashboards

This group covers the shared, real-time operational view that commanders and field units rely on to understand what is happening. It includes a centralised dashboard and interactive map that consolidates alerts, incidents, units/assets, POIs, evacuation layers, congestion, and connectivity blind spots. The focus is on consistent COP sharing across agencies, dynamic synchronisation (no manual refresh), and a usable interface that supports both tactical operations and strategic KPI monitoring.

2. Crowd monitoring & analytics

This group addresses the capability to observe, measure, and anticipate crowd dynamics in real time. It includes AI-driven video/sensor analytics for detecting abnormal patterns (panic, surges, counterflows, bottlenecks), generating density heatmaps, and forecasting crowd evolution. It also covers alerting and operator qualification of AI detections, plus real-time evacuation routing and proactive recommendations to prevent unsafe densities and uncontrolled crowd movements.

3. Geolocation, tracking & geofencing

This group focuses on precise positioning and movement tracking for responders, assets, and (where lawful) suspects, across indoor and outdoor environments. It includes accurate indoor location (including floor identification), automatic position updates (reducing radio reporting), and the ability to correlate geolocation with CCTV/sensor data. It also includes geofencing to detect restricted-area breaches and trigger immediate alarms.

4. Drone & anti-drone management

This group covers the functions needed to detect, classify, track, and manage drone threats in and around protected areas. It includes a dedicated anti-drone module, integration with authorised counter-UAS measures (e.g., lawful mitigation systems), and the fusion of drone telemetry/trajectories with responder positions and crowd density maps to predict risk/impact zones. The emphasis is on a unified aerial picture integrated into the overall operational environment.

5. Behavioural threat detection

This group targets the detection of violent or hazardous behaviours and coordinated hostile activity, using AI analytics that can operate even without biometric identification. It includes identifying weapon-like objects, coordinated groups, concealed faces, and behavioural indicators of aggression or attack preparation. The goal is early warning that feeds into anomaly/surge models while remaining aligned with GDPR and ethical AI constraints.

6. Logging, post-incident analysis & evidence

This group ensures the system can produce a reliable operational record of what happened, when, and why decisions were taken. It covers decision/action logging with rich metadata (timestamps, users, sources, components), secure tamper-proof storage, and automated generation of post-incident reports summarising timelines, communications, and outcomes. It supports accountability, lessons learned, and evidence handling under controlled access.

7. Architecture & interoperability

This group defines the system's technical foundations: open, modular design; standards-based protocols; and well-documented, versioned APIs to connect agencies and legacy systems without disrupting workflows. It includes middleware to bridge proprietary formats, unified time synchronisation, and broad support for common file/media formats. The aim is long-term scalability and integration readiness across heterogeneous ecosystems.

8. Public information & alerting

This group covers tools to inform and guide the public safely during incidents, across multiple channels (PA/loudspeakers, screens, apps, SMS, web, official channels). It includes geo-targeted alerts, multilingual and accessible messaging (including disability adaptation), and strict governance: messages can be auto-prepared but must require explicit human approval before dissemination, with full logging of the message lifecycle.

9. Multimedia intelligence & VMS

This group addresses the secure handling and sharing of video and multimedia intelligence across agencies. It includes compatibility with common VMS platforms, support for reliable video streaming formats, and sufficient bandwidth/priority for critical visual information. It also includes operationally concise metadata to make shared media quickly actionable and searchable within the joint environment.

10. Decision support & AI

This group focuses on AI-enabled capabilities that help decision-makers prioritise, predict, and recommend actions under time pressure—without replacing human authority. It includes predictive dashboards (incident evolution, resource needs, bottlenecks), threat prioritisation, response recommendations, anomaly/risk detection, and continuous learning from past operations and operator feedback. Usability and speed are core, ensuring outputs are interpretable and actionable.

11. Multi-agency platform & deployment

This group defines the platform as a shared operational environment for multiple organisations, supporting real-time information exchange and secure synchronised communications. It includes progressive onboarding (start small, scale to more agencies), and a federated integration model that avoids forcing a single system replacement. The goal is a deployable, scalable joint platform that supports both co-located centres and distributed operations.

Funded by the European Union

12. Command hierarchy & workflows

This group covers the digital representation and execution of command structures, responsibilities, and operational procedures. It includes modelling the chain of command, decision precedence, predefined intervention orders, and workflow routing for tasks, notifications, approvals, and escalations. It also includes automated escalation of critical alerts and AI-generated workflow proposals aligned with governance and SOPs.

13. Data integration & fusion

This group addresses ingesting and combining data from diverse sources—CCTV, drones, radars, sensors, reports, user inputs—into a coherent, real-time operational picture. It includes real-time upload and visualisation, interoperability of crowd-control data, and fusion of environmental indicators (sound/smoke/heat) with video to detect early triggers. It also includes simulation and pseudonymised views to rehearse coordination without exposing real operational data.

14. Access control & data governance

This group ensures the platform enforces who can see and do what, across agencies and roles. It includes RBAC, multi-level data sharing controls, hierarchy-based view restrictions, and RBAC-aware integration so shared workflows can run without violating confidentiality. It explicitly targets strict segregation and compliance with security and data protection requirements.

15. Performance & latency

This group sets expectations for real-time operational performance. It includes end-to-end latency targets for COP updates, throughput for high-volume multimodal data, and geospatial mapping quality (resolution, accuracy, rendering). It also covers usability under time pressure, ensuring that critical information remains readable, responsive, and stable during peak operational load.

16. Communications & networks

This group covers the secure, resilient communications backbone needed to sustain operations in hostile or overloaded conditions. It includes encrypted, high-speed data exchange; redundancy and failover across heterogeneous networks (TETRA/LTE/5G/satellite); overload management; detection of degraded comms; anti-jamming/spectrum monitoring; secure key management; and secure mobile/public alerting capabilities (including cell broadcast where applicable). The focus is on continuity, integrity, and interoperability across agencies.

Funded by the European Union