

3 de septiembre de 2021

Estimados amigos:

A través de este nuevo boletín informativo, os hacemos llegar las últimas novedades del

**Clúster 3: Seguridad civil para la sociedad**

- **CERIS (Community of European Research and Innovation in Security) WORKSHOP ON DISASTER RISK REDUCTION AND SPACE-BASED APPLICATIONS, 15 SEPTEMBER 2021.**

*The dramatic flooding event that occurred in Germany and Belgium on the 15-16 July 2021, affecting also neighbouring countries, has highlighted a clear gap between available scientific information and impact forecasting tools and the timely communication and consideration of related warnings by local authorities, which resulted in an insufficient capacity to evacuate people at risk. This gap sadly reflects the insufficient understanding by local authorities and populations of risk exposure for this type of extreme events (exacerbated by climate change), as well as a lack of clear governance mechanism to react to sudden extreme events. This requires a cross-sectoral, cross-border, cross-disciplines integrated approach as well as a full risk awareness at all levels, including by citizens.*

*In this respect, based on recommendations made by civil protection experts, policy-makers and the scientific community, the Horizon Europe Cluster 3 Disaster-Resilience Societies for Europe thematic area (DRS) has issued several topics on integrated disaster risk reduction (DRR) aspects. These topics recognise that, besides modelling and impact forecasting tools available to date, space-based applications have a strong role to play in DRR, for instance for tracking the evolution of forest fires or convective clouds precursors of flash floods. Within the 2021 Horizon Europe call, four DRS topics therefore indicate that “if projects use satellite-based, positioning, navigation and/or related timing data and services, they must make use of Galileo/EGNO, as well as other data and services, while the use of Copernicus for earth observation is encouraged”. In this regard, and in order to clarify and facilitate interactions among the DRR and spatial communities, **DG HOME will organise a workshop in the framework of the Community for European Research and Innovation for Security (CERIS) on the 15th September 2021, 10h-12h30.** In this context, discussions will turn around the DRS topics, inviting experts to express their view about the scope of the research actions and their links to space-based applications.*

The registration is now open: [https://ec.europa.eu/eusurvey/runner/DRS\\_space](https://ec.europa.eu/eusurvey/runner/DRS_space)

- **Nuevas dos newsletters del proyecto SEREN4 – red de puntos nacionales de contacto de I+D+i en seguridad.**

Contiene información sobre el acceso a las grabaciones y presentaciones del Infoday Europeo sobre la convocatoria 2021, que tuvo lugar los días 30 de junio y 1 de julio, la búsqueda de socios y otros programas de financiación Europeos relacionados. Ver Anexo 1.

Contiene información sobre: la gestión y requisitos de los proyectos que impliquen información clasificada, los aspectos sociales, éticos y la Inteligencia artificial en los proyectos del clúster 3, así como la participación de Suiza en Horizonte Europa, entre otros temas. Ver Anexo 2.

- **Jornada informativa Europea sobre las convocatorias del programa EDF (2021): Del 15 al 17 de septiembre de 2021**, la Comisión Europea organizará un día de información virtual y un evento de networking para los posibles solicitantes de las convocatorias de propuestas del Fondo Europeo de Defensa (FED) 2021.

Para información e inscripción pinche el siguiente enlace: [European Defence Fund \(EDF\): Information Day & Networking Event \(europa.eu\)](https://europa.eu/edf-information-day)

- **Cybersecurity@CEPS Summit, 2021 – 1 y 2 de diciembre de 2021.** “ Building cyber resilience for a sustainable post pandemic recovery”. Más información e inscripciones en: [Cybersecurity@CEPS Summit 2021 – CEPS](https://ceps-summit.com)

- **Búsquedas de socios convocatoria 2021 Clúster 3:**

- **Propuesta coordinada por entidad de Estonia interesada en incorporar usuarios finales** (topic: HORIZON-CL3-2021-BM-01-04: Advanced detection of threats and illicit goods in postal and express courier flows). Más información en Anexo 3.
- **Entidad italiana interesada en participar en una propuesta del topic:** FCT-01-07 Improved preparedness on attacks to public space. Ver Anexo 4.
- **Entidad británica interesada en incorporarse a algún consorcio para el topic:** HORIZON-CL3-2021-BM-01-02: Increased safety, Security, performance of the

European Border and Coast Guard and of European customs authorities. Más información en Anexo 5.

- **Entidad británica interesada en incorporarse en alguna propuesta para el topic:** CS-01-03: AI for Cybersecurity Reinforcement. Más información en Anexo 6.
- **Entidad británica interesada en unirse a algún consorcio en los topics siguientes:** DRS-01, DRS-02, DRS-03 y SSRI 02. Más información en Anexo 7.
- **Entidad británica con experiencia en el área SSH, interesada en integrarse en alguna propuesta para la convocatoria FCT 2021.** Más información en Anexo 8.

Esperamos que esta información os resulte de interés.

Un cordial saludo,

*Maite Boyero Egido*

*Representante y Punto de Contacto Nacional Clúster 3*

*Departamento de Retos Sociales. Dirección de Programas Europeos y Cooperación Territorial*

*Centro para el Desarrollo Tecnológico Industrial, E.P.E.*

*C/Cid, 4. 28001 Madrid*

*maite.boyero@cdti.es, +3491 581 5562*

# Horizon Europe Cluster 3 Open Calls

## Content

- A. Overview of the currently open calls ..... 1
- B. Useful Information ..... 5
  - I want more information about the open calls and topics..... 5
  - I am looking for partners and expertise to build consortium, where to find them? ..... 6
  - Is there any other useful workshop or seminar I should be aware of? ..... 6
  - Is there any platform gathering civil security stakeholders managed by the European Commission?..... 6
  - Are there any other relevant programmes or initiatives? ..... 7

### A. Overview of the currently open calls

[Link](#) to the pdf version of the Work Programme

[Direct link](#) to Funding and Tender Portal (open topics under Cluster 3)

Destination	Area	ID	Topic	Call open	Call closed	Type of action	Budget per project/ mil. EUR	Budget per projects/ mil. EUR	TRL
Better protect the EU and its citizens	Modern information analysis for fighting crime and terrorism	FCT01	<i>FCT-2021-01-01: Terrorism and other forms of serious crime countered using travel intelligence</i>	30.6.	23.11.	IA	5	16	6-7
		FCT01	<i>FCT-2021-01-03: Disinformation and fake news are combated and trust in the digital world is raised</i>	30.6.	23.11.	IA	4		6-7



Destination	Area	ID	Topic	Call open	Call closed	Type of action	Budget per project/ mil. EUR	Budget per projects/ mil. EUR	TRL
		FCT01	<i>FCT-2021-01-04: Improved access to fighting crime and terrorism research data</i>	30.6.	23.11.	IA	7		7-8
		FCT01	<i>FCT-2021-01-02: Lawful interception using new and emerging technologies (5G &amp; beyond, quantum computing and encryption)</i>	30.6.	23.11.	RIA	5	5	5-6
	Improved forensics and lawful evidence collection	FCT02	<i>FCT-2021-01-05: Modern biometrics used in forensic science and by police</i>	30.6.	23.11.	IA	5	5	6-7
	Enhanced prevention, detection and deterrence of societal issues related to various forms of crime	FCT03	<i>FCT-2021-01-06 – Domestic and sexual violence are prevented and combated</i>	30.6.	23.11.	IA	3	6	6-7
	Increased security of citizens against terrorism, including in public spaces	FCT04	<i>FCT-2021-01-07: Improved preparedness on attacks to public spaces</i>	30.6.	23.11.	IA	3	3	6-7
	Organised crime prevented and combated	FCT05	<i>FCT-2021-01-08: Fight against trafficking in cultural goods</i>	30.6.	23.11.	RIA	5	5	5-6
		FCT05	<i>FCT-2021-01-09: Fight against organised environmental crime</i>	30.6.	23.11.	IA	5	10	6-7
		FCT05	<i>FCT-2021-01-10: Fight against firearms trafficking</i>	30.6.	23.11.	IA	5		6-7
	Citizens are protected against cybercrime	FCT06	<i>FCT-2021-01-11: Prevention of child sexual exploitation</i>	30.6.	23.11.	RIA	3	6	n/a
		FCT06	<i>FCT-2021-01-12: Online identity theft is countered</i>	30.6.	23.11.	RIA	3		5-6
Effective management of EU external borders (BM)	Efficient border surveillance and maritime security	BM01	<i>BM-2021-01-01: Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support</i>	30.6.	23.11.	IA	7	7	7-8
	Secured and facilitated crossing of external borders	BM02	<i>BM-2021-01-02: Increased safety, security, performance and comfort of the European Border and Coast Guard and of European custom authorities</i>	30.6.	23.11.	CSA	2,5	2,5	n/a



Destination	Area	ID	Topic	Call open	Call closed	Type of action	Budget per project/ mil. EUR	Budget per projects/ mil. EUR	TRL
	Better customs and supply chain security	BM02	<i>BM-2021-01-03: Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff</i>	30.6.	23.11.	IA	4	8	7-8
		BM03	<i>BM-2021-01-04: Advanced detection of threats and illicit goods in the postal and express courier flows</i>	30.6.	23.11.	RIA	4	8	4-6
		BM03	<i>BM2021-01-05: Improved detection of concealed objects on, and within the body of, persons</i>	30.6.	23.11.	IA	5	5	7-8
Resilient Infrastructure	Improved preparedness and response for large-scale disruptions of European infrastructures	INFRA01	<i>INFRA-2021-01-01 European infrastructures and their autonomy safeguarded against systemic risks</i>	30.6.	23.11.	IA	10	20	6-7
		INFRA01	<i>INFRA-2021-01-02: Ensured infrastructure resilience in case of Pandemics</i>	30.6.	23.11.	IA	10		6-7
Increased Cybersecurity (CS)	Secure and resilient digital infrastructures and interconnected systems	CS01	<i>CS-2021_01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity</i>	30.6.	21.10.	RIA	3-5	21,5	4
	Hardware, software and supply chain security	CS02	<i>CS-2021-01-02 Improved security in open-source and open-specification hardware for connected devices</i>	30.6.	21.10.	RIA	3-5	18	4
	Cybersecurity and disruptive technologies	CS03	<i>CS-2021-01-03: AI for cybersecurity reinforcement</i>	30.6.	21.10.	RIA	3-4	11	4
	Human-centric security, privacy and ethics	CS05	<i>CS-2021-01-04: Scalable privacy-preserving technologies for data spaces in Europe involving personal data</i>	30.6.	21.10.	RIA	3-5	17	4
A Disaster-Resilient Society for Europe	Societal Resilience: Increased risk Awareness and preparedness of citizens	DRS01	<i>DRS-2021-01-01: Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards</i>	30.6.	23.11.	RIA	5	5	n/a
	Improved Disaster Risk Management and Governance	DRS02	<i>DRS-2021-01-02: Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long</i>	30.6.	23.11.	IA	6	6	n/a



Destination	Area	ID	Topic	Call open	Call closed	Type of action	Budget per project/ mil. EUR	Budget per projects/ mil. EUR	TRL
			<i>term adaptation and resilience building</i>						
		<b>DRS02</b>	<i>DSR-2021-01-03: Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections</i>	30.6.	23.11.	RIA	5	5	n/a
		<b>DRS02</b>	<i>DRS-2021-01-04: Developing a European partnership to coordinate R&amp;I efforts on land management and climate-related disasters</i>	30.6.	23.11.	CSA	2	2	n/a
		<b>DRS02</b>	<i>DRS-2021-01-05: Fast deployed mobile laboratories to enhance situational awareness for pandemics and emerging infectious diseases</i>	30.6.	23.11.	IA	4	8	6-8
<b>SSRI (Strengthened Security Research and Innovation)</b>	<b>Stronger pillars of security Research and Innovation</b>	<b>SSRI 01</b>	<i>SSRI-2021-01-01: A maturity assessment framework for security technologies</i>	30.6.	23.11.	RIA	1,5	1,5	n/a
		<b>SSRI 01</b>	<i>SSRI-2021-01-02: Knowledge Networks for Security Research &amp; Innovation</i>	30.6.	23.11.	CSA	2	4	n/a
		<b>SSRI 01</b>	<i>SSRI-2021-01-03: National Contact Points (NCPs) in the field of security and cybersecurity</i>	30.6.	23.11.	CSA	2,5	2,5	n/a
	<b>Increased Innovation uptake</b>	<b>SSRI 02</b>	<i>SSRI-2021-01-04: Demand-led innovation for situation awareness in civil protection</i>	30.6.	23.11.	PCP	6	6	6-8
	<b>Cross-cutting knowledge and value for common security solutions</b>	<b>SSRI 03</b>	<i>SSRI-2021-01-05: Societal Impact assessment and impact creation transdisciplinary methods for security research technologies driven by active civil society engagement</i>	30.6.	23.11.	RIA	2	2	n/a



## B. Useful Information

I want more information about the open calls and topics...

- ✓ **Horizon Europe Civil Security for Society Infoday** (30 June 2021)

The event was recorded, and you can access the recording via the [event's website](#). As the [recording](#) covers the whole Information Day, we have decided to provide you with the timing of different sessions in the list below (hh:mm – hh:mm):

- 1) Introduction to Cluster 3 (video time 0:22-0:35)
- 2) Operational aspects and novelties in HE (video time 0:35 - 1:15)
- 3) Paving the pathways to IMPACT (video time 1:20 – 1:37)
- 4) Legal and financial issues (video time for legal part 2:00 –2:30; time for financial part 2:30- 2:42)
- 5) Ethics and Integrity in HE (video time : 2:42 - 2:56)
- 6) Security Appraisal, security and classified information and implementation of the security requirements in GA: (video time: 2:57– 3:24)
- 7) Exploitation and dissemination – novelty in HE: (video time - 4:07 - 4:20)
- 8) Gender issues (video time - 4:24 - 4:35)
- 9) SSH in Cluster 3 proposals (video time - 4:52 – 5:02)
- 10) CERIS – video (video time - 4:39 – 4:51)
- 11) BM- Border management (video time - 5:04 - 5:29)
- 12) SSRI - (video time - 5:30 – 5:55)
- 13) FCT - (video time - 6:07 - 6:53)
- 14) DRS - (video time - 6:55 - 7:28)
- 15) INFRA - (video time – 7:30 – 7:58)
- 16) CS - Cybersecurity (video time - 7:58 – 8:35)

Find the presentations for the Information Day:

- [General Information on Cluster 3 in Horizon Europe](#)
- [Legal and Financial Aspects](#)
- [Community for European Research and Innovation for Security \(CERIS\)](#)
- [Cross-cutting Issues: Gender/SSH](#)
- [Cluster 3 - Border Management Call](#)
- [Cluster 3 - Strengthened Security Research and Innovation call](#)
- [Cluster 3 - Fighting Crime and Terrorism call](#)
- [Cluster 3 - Disaster-Resilient Society for Europe Call](#)
- [Cluster 3 - Resilient Infrastructures](#)
- [Cluster 3 - Increased cybersecurity](#)

- ✓ Visit [SEREN4](#) website and [Funding and Tenders Portal](#) to get relevant information.





I am looking for partners and expertise to build consortium, where to find them?

- ✓ **Horizon Europe Civil Security for Society Brokerage event** (1 July 2021)  
[Download the presentations](#) from the pitch session  
[Arrange bilateral meetings](#) until 19 November 2021

Some statistical figures about the currently open brokerage event:

- 1300+ company and organization profiles
- 400+ published collaboration opportunities
- 500+ 1:1 meeting requests sent

- ✓ **SMi2G Event 2021** (31 May – 1 June 2021)  
[Download the presentations](#) from the pitch session (project ideas, profiles and expertise of participants), take a look and read the collaboration offers.

- ✓ Contact your [National Contact Point](#) (NCP)

Is there any other useful workshop or seminar I should be aware of?

- ✓ **FRONTEX and Cluster 3** (1 July 2021), workshop relevant to Border management topics  
[Recording](#)
- ✓ **Workshop and Q&A on Impact aspects in Horizon Europe** in Cluster 3 (1 July 2021)  
[Recording](#)
- ✓ **Dissemination & Exploitation in Horizon Europe**, EC Webinar (9 June 2021)  
[Presentations and Recording](#)
- ✓ **A successful proposal for Horizon Europe: Scientific-technical excellence is key, but don't forget the other aspects**, EC Webinar (21 April 2021)  
[Presentations and Recording](#)

Is there any platform gathering civil security stakeholders managed by the European Commission?

- ✓ **CERIS - Community for European Research and Innovation for Security**

CoU - Community of Users for Safe, Secure and Resilient Societies that represents informal platform with around 1500 registered stakeholders has enlarged its scope and became the [Community for European Research and Innovation for Security \(CERIS\)](#).

[contact@seren-project.eu](mailto:contact@seren-project.eu)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786680

The objectives of CERIS are to:

- analyse identified **capability needs and gaps** in the corresponding areas;
- identify **solutions** available to address the gaps;
- translate capability gaps and potential solutions into **research needs**;
- identify **funding opportunities and synergies** between different funding instruments;
- identify **standardisation** research-related needs;
- integrate the **views of citizens**;

Thematic areas:

1. Border management (BM)
2. Disaster resilient societies (DRS)
3. Fighting crime and terrorism (FCT), incl. infrastructure protection
4. Strengthened security research and innovation (SSRI)

Are there any other relevant programmes or initiatives?

- ✓ **Internal Security Fund Programme (ISF)**: With an overall budget of EUR 1.9 billion, the Internal Security Fund, will finance actions in the field of fight against terrorism and radicalization, serious and organized crime, cybercrime and the protection of victims.
- ✓ **Border Management and Visa Instrument (BMVI)**: With an overall budget of EUR 6.4 billion, the Border Management and Visa Instrument, contributes to securing strong EU external borders, which in turn will allow the EU to maintain a Schengen area without internal border controls.
- ✓ **European Defence Fund (EDF)**: The Fund will financially support consortia of companies from different member states undertaking cooperative defence research and development of defence products and technologies. EDF has a budget of EUR 7,9 billion over 2021-2027.
- ✓ **Digital Europe Programme (DIGITAL)**: The Programme will provide funding for projects in five crucial areas: supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and ensuring the wide use of digital technologies across the economy and society with a budget of EUR 7.6 billion from 2021 to 2027.
- ✓ **European Cybersecurity Competence Centre and Network**: The European Cybersecurity Competence Centre (ECCC) aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community.



## Content

1.	Useful documents for the proposal preparation .....	2
1.1.	Programme Security Instruction for Horizon Europe .....	2
1.2.	Classification of information in Horizon Europe projects .....	2
1.3.	How to handle security-sensitive projects .....	2
1.4.	Proposal template: Part B Security Section .....	2
1.5.	Security Scrutiny .....	3
1.6.	Guidance notes for misuse of research results .....	3
1.7.	Annotated Model Grant Agreement .....	3
1.8.	Ethics guide: How to complete your ethics self-assessment .....	4
2.	EC proposal of the Artificial Intelligence systems “AI Regulation” .....	4
3.	Participation of Switzerland in Horizon Europe Programme .....	6
4.	Galileo/EGNOS and/or Copernicus .....	6
5.	Social Sciences and Humanities - SSH .....	7
6.	Cascade Funding.....	8

# 1. Useful documents for the proposal preparation

Below you can find some information that we consider useful for the preparation of your proposal.

## 1.1. Programme Security Instruction for Horizon Europe

[Programme Security Instruction for Horizon Europe](#) (PSI) represents 81 pages of helpful information. This PSI establishes the security procedures to be applied and the standard security procedures and processes to be followed to manage a classified grant awarded under the Horizon Europe Programme, as well as assigns the responsibilities for the protection of classified information generated or exchanged in connection with the Programme.

## 1.2. Classification of information in Horizon Europe projects

[Classification of information in Horizon Europe projects](#) was initially published in 2013. This updated guide explains when and for how long the information has to be classified, the different classification levels and how to classify information in different cases of research (explosive, CBRN, critical infrastructures, terrorism, boarder security, organised crime, digital security and space).

## 1.3. How to handle security-sensitive projects

[How to handle security-sensitive projects](#) guide covers proposal stage, grant preparation stage and the Horizon Europe project implementation. EU classification is normally needed if activity concerns a security-sensitive subject matter and falls under one of the security-sensitive types of activities. **The precise details and cases vary by EU Programme.** For more information and examples, see the Guidelines on the classification of information in Horizon Europe projects, classification of information in Digital Europe projects and classification of information in European Defence Fund projects.

## 1.4. Proposal template: Part B Security Section

The Security Section of the [proposal template Part B](#) must be completed in accordance with the guidance [How to handle security-sensitive projects](#) and [Classification of information in Horizon Europe projects](#). The form also includes instructions for preparing a Security Aspects Letter (SAL).

- **Security Aspect Letter (SAL):** if your project intends to use or produce classified information, you have to fill in the SAL (a part of proposal template in security section),



according to your project-specific security requirements. Consult the guidance Classification of information in Horizon Europe projects. The security aspects letter (SAL) is an integral part of the classified grant agreement and describes grant agreement specific security requirements.

- **Security Classification Guide (SCG)**: is a document (Annex of the SAL) which describes classified elements of a project or a grant agreement (deliverables) specifying the applicable security classification levels. The SCG lists classified deliverables as defined in a security scrutiny procedure. The SCG issued to Beneficiaries may be modified throughout the life of the grant agreement and the classified elements may be re-classified or downgraded. The SCG also includes, if applicable, an informative list of Classified Background Information used.

## 1.5. Security Scrutiny

[Security Scrutiny](#) ensures sufficient protection of classified information in EU grants. It is implemented for projects selected for funding. If the scrutiny leads to requirements to be implemented before grant signature, you will need to take immediate action to comply. If the scrutiny leads to classification and additional requirements to be fulfilled during the project, this will be automatically reflected in the system (classification of existing deliverables, Security Aspect Letter (SAL), Security Classification Guide (SCG), additional security deliverables and security requirements work package).

## 1.6. Guidance notes for misuse of research results

[Guidance notes for misuse of research results](#) will be available soon.

## 1.7. Annotated Model Grant Agreement

[Annotated Model Grant Agreement](#) (AGA) is a user guide that aims to explain to applicants and beneficiaries the EU Model Grant Agreements (General MGA, Lump Sum MGA, Unit MGA, Operating Grants MGA and Framework Partnership Agreement) for the EU funding programmes 2021-2027.

Programme specificities are reflected in this document as examples — in so far as they are accepted as mainstream solutions that can be used by several EU programmes. The purpose of this document is to help users understand and interpret their Grant Agreements (GAs). By avoiding technical vocabulary, legal references and jargon, it seeks to help readers find answers to the practical questions they may come across when setting-up or implementing their projects. In the same spirit, the document's structure mirrors that of the EU Model Grant Agreements (MGAs). It explains each MGA Article and includes examples where appropriate.



## 1.8. Ethics guide: How to complete your ethics self-assessment

A new version of the Ethics guide: [How to complete your ethics self-assessment](#) is available on the Funding and Tender Opportunities Portal. Data for Digital Europe programme and European Defence Fund were integrated. The Ethics Guide now also includes a section on Artificial Intelligence solutions in projects. It explains the basic principles of its ethical use. It also refers to the [Ethics Guidelines for Trustworthy AI](#) (available in all languages) prepared by independent experts. In this context, we draw your attention to the draft of the new “AI Regulation”, described separately in this Newsletter.

Information about [Key changes to the ethics appraisal process](#) in HE can be obtained at an interesting EC workshop (130minutes), where 40 minutes are devoted to the issue of ethics in the use of artificial intelligence.

## 2. EC proposal of the Artificial Intelligence systems “AI Regulation”

On 21 April 2021, the European Commission (EC) published its proposal for a [Regulation on Artificial Intelligence](#) (the "AI Regulation"). This proposal results from several years of work of the European Commission, including a "[White Paper on Artificial Intelligence](#)" and broad public consultation. We wrote about the initial documents on AI in the [SEREN4 Newsletter, April 2020](#). Furthermore, the EC proposal is based on the EU Parliament's October 2020 legislative proposal to create a legal and ethical framework/rules for the rapid development and deployment of AI.

The proposal contains recommendations for several regulatory measures and definitions of the terminology used. It aims to establish a legal framework necessary to facilitate innovation and investment in AI. Furthermore, the new Regulation should ensure safe and trustworthy use of AI applications while maintaining a code of ethics.

The main provisions of the AI Regulation are the introduction of:

- **Binding rules** for AI systems that apply to providers, users, importers, and distributors of AI systems in the EU, irrespective of where they are based;
- A list of specific **prohibited** AI systems;
- Extensive **compliance obligations** for high-risk AI systems;

Article 3 of the General Provision brings definitions of the **terminology** used, for example:

- **Artificial intelligence system** (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;



- **Intended purpose** means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;
- **Reasonably foreseeable misuse** means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;
- **Training data** means data used for training an AI system through fitting its learnable parameters, including the weights of a neural network;
- **Validation data** means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split;
- **Testing data** means data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service; of undermining fundamental rights and are therefore explicitly prohibited;
- **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Examples of other listed term: biometric categorisation system; remote biometric identification system; real-time remote biometric identification system; publicly accessible space; serious incident and many other.

Title II, Article 5 - **Prohibited AI practices** - The proposed AI Regulation lists several AI systems which EC believe bear an unacceptable risk of violating fundamental rights and are therefore explicitly prohibited (ethical consideration). The Regulation contains a proposal for exemptions for LEAs (specific cases of real-time remote biometric identification systems in publicly accessible spaces).

Title III of the Regulation regards **High-risks AI** systems and proposes an approach for their classification and the criteria for the quality and working with data used or generated in these high-risk AI systems and training. The Regulation also contains conditions for technical documentation, record-keeping, transparency and provision of information to users. The proposal also sets out the purpose and requirements for human oversight and covers high-risk AI systems' accuracy, robustness, and cybersecurity. Eight areas of high-risk AI systems use are listed in Annex III of the AI Regulation.

Of course, the proposed AI Regulation has a much broader scope with implications for innovation and future markets. In this article, we have selected only parts where we want to draw the attention of research projects proposers. We consider them essential because the AI systems resulting from the currently prepared projects will be put into practice when the AI regulation is binding.



### 3. Participation of Switzerland in Horizon Europe Programme

Entities based in Switzerland can participate in Horizon Europe. However, as Switzerland is considered a non-associated country, Swiss entities (including companies and SMEs) can apply only for Horizon Europe's calls and related programmes and initiatives open to non-associated third country participation.

Legal entities taking part in collaborative projects open to third country participation will receive funding via the State Secretariat for Education, Research and Innovation (SERI) in the same way as it was organised in the past. In addition, a corresponding financial guarantee, which can be shared with the consortium partners, is provided by SERI on its [website](#).

In the new generation of EU Programmes for Research and Innovation, entities from non-associated third countries participate in the collaborative projects as associated partners. The budget of the associated partner is indicated in the project proposal but not taken into account in the project budget and corresponding EC funding.

Participants from non-associated third countries cannot coordinate projects. They can, however, lead work packages as any other participant.

We highly recommend consulting the participation of Switzerland in the 2021 calls for the collaborative proposals with the documents provided by SERI as these documents are constantly updated:

- Information on the [Swiss participation in H2020 and HE](#)
- [Questions and Answers](#) on the Swiss participation in H2020 and HE

### 4. Galileo/EGNOS and/or Copernicus

In more than 100 topics across Horizon Europe Clusters for 2021-2022 calls, the use of EGNOS and/or Copernicus services and data is considered necessary. Therefore, if projects use the navigation, positioning and other services, including remote sensing, the European Commission mandates the involvement of the European Galileo / EGNOS and Copernicus systems. Galileo/EGNOS and Copernicus data and services are free of charge.

There are 25 such topics in Cluster 3 Work Programme 2021-2022 with the following eligibility condition:

“If projects use satellite-based, positioning, navigation and/or related timing data and services, beneficiaries must make use of Galileo/EGNOS (other data and services may additionally be used). The use of Copernicus for earth observation is encouraged.”





Cluster 3 Work Programme 2021 with Galileo/EGNOS eligibility condition:

TOPIC
HORIZON-CL3-2021-FCT-01-07: Improved preparedness on attacks to public spaces
HORIZON-CL3-2021-FCT-01-08: Fight against trafficking in cultural goods
HORIZON-CL3-2021-FCT-01-09: Fight against organised environmental crime
HORIZON-CL3-2021-FCT-01-10: Fight against firearms trafficking
HORIZON-CL3-2021-BM-01-01: Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support
HORIZON-CL3-2021-BM-01-02: Increased safety, security, performance of the European Border and Coast Guard and of European customs authorities
HORIZON-CL3-2021-BM-01-03: Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff
HORIZON-CL3-2021-DRS-01-01: Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards
HORIZON-CL3-2021-DRS-01-02: Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building
HORIZON-CL3-2021-DRS-01-03: Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections
HORIZON-CL3-2021-DRS-01-06: Fast deployed mobile laboratories to enhance situational awareness for pandemics and emerging infectious diseases

## 5. Social Sciences and Humanities - SSH

Assessing the effective contribution of social science and humanities disciplines and expertise is, in some cases, part of the scientific methodology of the project.

When the integration of SSH is required, applicants have to show the roles of these disciplines or justify if they consider that SSH is not relevant for their project. A proposal without a sufficient contribution/integration of SSH research and competencies will receive a lower evaluation score.

Cluster 3 – WP 2021 - topics flagged as SSH relevant:

TOPIC
HORIZON-CL3- 2021- CS- 01- 01 Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity
HORIZON-CL3-2021-FCT-01-06 Domestic and sexual violence are prevented and combated
HORIZON - CL3 2021 FCT 01-07 Improved preparedness on attacks to public spaces
HORIZON - CL3 2021 FCT 01 08 Fight against trafficking in cultural goods
HORIZON-CL3- 2021- FCT -01-11 Prevention of child sexual exploitation

HORIZON-CL3 -2021-FCT-01 -12 Online identity theft is countered
HORIZON-CL3 -2021- DRS- 01- 01 Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards
HORIZON-CL3 -2021-DRS -01 -02 Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building
HORIZON-CL3- 2021-DRS- 01- 03 Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections
HORIZON-CL3-2021- SSRI -01 -02 Knowledge Networks for Security Research & Innovation
HORIZON-CL3- 2021- SSRI -01- 05 Security research technologies driven by active civil society engagement: transdisciplinary methods for societal impact assessment and impact creation

## 6. Cascade Funding

Cascade Funding in Horizon Europe, also known as [Financial Support for Third Parties](#) (FSTP), is a European Commission mechanism to distribute funding from the project consortia to the third parties, mainly SMEs, to uptake or develop innovative digital technologies.

Cluster 3 cybersecurity calls 2022 ([CS-2022-01-01](#) and [CS-2022-01-03](#) ) involve possible implementation of FSTP mechanism, in which consortia may publish their own calls for proposals (open calls) and provide financial support in the form of grants. Cascade funding also occurs in other Clusters, but most typically in calls of Cluster 4 (Digital, Industry and Space).



## Invitation to the consortium

### Reduce the risks in e-commerce combining cosmic ray scanners and AI-based technologies

**Call:** [HORIZON-CL3-BM-2021-01-04: Advanced detection of threats and illicit goods in the postal and express courier flows](#)

**Budget:** 4 M € per project, 100 % financed by the EC

**Submission deadline:** 23<sup>rd</sup> of November 2021

We invite you to participate as a member of this consortium.

Parcel delivery is a very fast-growing domain, which is driven by e-commerce applications and accelerated by the Covid-19 pandemic outbreak in 2020. Despite many benefits, the use of postal or courier-borne devices for transporting illicit goods is a well-known tactic of terrorists and criminal groups.

The currently available and widely used x-ray technologies to detect illicit goods have certain limitations, like shielding possibilities and lack of effective automated recognition. Only small fractions of parcels are scanned at delivery centres and efficiency of detection is very low. Cosmic ray tomography systems have high potential to solve these problems with their more sensitive material discrimination, superior penetration capabilities, thus overcoming malicious concealments, enabling better detection.

This led us to the idea to develop a tomographic scanning technology combined with AI-based risk assessment for parcel delivery centres. During the project we will develop a prototype scanner and an AI-based risk management system. The technology allows fully automated threat detection and decision-making processes for a large number of postal packages simultaneously. The project outcome is a module-based scanner system installed at a parcel delivery centre's facility and testing it together with the risk management system.

Please contact me to discuss this amazing opportunity further. We look forward to a positive collaboration on this project.

Andi Hektor ([andi.hektor@gscan.eu](mailto:andi.hektor@gscan.eu))

### Confirmed consortium members

No	Name	Country	Sector	Role
1.	<a href="#">GScan OU</a>	Estonia	Industry	Technology provider
2.	<a href="#">VTT</a>	Finland	Research	Research provider
3.	<a href="#">FBK</a>	Italy	Research	Research provider
4.	<a href="#">TalTech</a>	Estonia	Academia	Research provider
5.	<a href="#">Estonian Customs</a>	Estonia	Customs authority	End-user/testing and validating
6.	<a href="#">Finnish customs</a>	Finland	Customs authority	Requirement analysis, validating

## PARTNER SEARCH UNDER HORIZON EUROPE CL3

### CALL: HORIZON-CL3-2021-FCT-01-07: Improved preparedness on attacks to public space

**ITSTIME research team of the Università Cattolica del Sacro Cuore** is looking for partners to submit a proposal under the topic HORIZON-CL3-2021-FCT-01-07: Improved preparedness on attacks to public space. Itstime has a specific area of research and activity that focuses mainly on terrorism and emergencies management. Specifically, on terrorism analysis, it develops threat assessments of terrorist attacks and evaluate success factors.

Given its expertise on such topics, ITSTIME can contribute to the topic HORIZON-CL3-2021-FCT-01-07: Improved preparedness on attacks to public space, specifically with regards to the prevention of terrorist attacks identifying vulnerabilities and windows of opportunity for attackers through trend and modus operandi analysis. In such context we can successfully develop:

- Mitigation strategies to improve vulnerability assessments and authorities' planning and strategic capabilities with a specific focus on countering and/or preventing terrorist attacks or other forms of severe violence;
- Best practices of risk management which involve LEA, society and institutions in preventing and countering terrorist attacks to identify specific vulnerabilities and elaborate mitigation strategies simulating attack scenarios in any public space in realistic conditions;
- Policies of space management that take into account the majority of strategical and security-related factors due to the identification of potential vulnerabilities connected to the design/refurbishment and construction/improvement of different public spaces.

### Who we are:

Founded in 1921, **Università Cattolica del Sacro Cuore (UCSC)** is the largest private university in Europe with 12 Faculties, 5 campuses across Italy (Milan, Rome, Piacenza, Cremona and Brescia), and about 41.000 students of which 2.395 are international students.

Research activity draws on 1293 tenured researchers, 39 departments, 1 institute 94 research centres, 6 university centres and 11 spin-offs and is aimed towards the study and understanding of crucial issues of life and society: new frontiers in economics and bioethics, changes in the field of law, family and cultural trends, mass media, changes in political systems, aims and goals of medicine, technological applications of mathematics and physics, and the most recent discoveries in environmental research.

UCSC boasts strong industrial and institutional ties that facilitate networking at national and international level, as well as collaborations in groundbreaking research projects, which generated about 4.500 scientific publications over the last year particularly in the fields of science innovations, environment and sustainability, and health.

UCSC is highly engaged in carrying out multidisciplinary research project both at national and international level. The annual average of research funds is 30M Euro, coming from UCSC own funds (10%), national grants and international grants (45%) and funds from applied research with private and public, national and international entities (45%).

Between 2014 and 2020 UCSC has participated in 70 Research and Innovation projects (11 as coordinator/host institution) funded by the European Commission under the Horizon 2020 Programme and in 74 projects (40 as coordinator/host institution) co-funded by other EU and international funding programmes. These projects cover several scientific areas (Humanities, Economics and Social Sciences, Security, Health, Food and Agriculture).

Further information:

<https://www.unicatt.it/>

<https://ricerca.unicatt.it/>

**ITSTIME - Italian Team for Security, Terroristic Issues & Managing Emergencies (<https://www.itstime.it/>)**, is the leading research team on security, terrorism and crisis management based at the Department of

Sociology of UCSC. ITSTIME is a “project” because it addresses both theoretically and empirically the new challenges in the post 9/11 world with a multidisciplinary approach promoting research focused on security issues from different perspectives. The missions of the project are threefold: to address security, intended as a condition that results from the establishment and maintenance of protective measures able to promote citizens' wellness and democratic vitality of the institutions; to deal with Terrorism, as a long-term threat that must be addressed through preventive and well-constructed measures; to Manage Emergencies to develop helpful practices both for citizens and institutions. **ITSTIME collaborates with public and private subjects** interested in monitoring emerging threats, elaborating potential risk scenarios, planning prevention strategies, developing plans for responding to emergencies. ITSTIME is **on the field** in several Countries: Afghanistan, Somalia, Syria, etc. At international level ITSTIME is member of the board of EENeT, European Expert Network on Terrorism, ICTAT -International Counter-Terrorism Academic Community and represents Italy in the project on. ITSTIME managed and participated **several competitive international research projects** in the last years: “COUNTER: Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalization and Citizen Protection (H2020, 2021-on going); Countering Violent Extremism Through Arts and Culture (UAE Ministry of Culture and Knowledge 2019-2020); Development Trivalent: Terrorism Prevention Via Radicalisation Counter-narrative (H2020, 2017-2020); From Criminals to Terrorists and Back (Globse 2017-2018); Stress: Strategies, Tools and new data for REsilient Societies (Cariplo Foundation, 2017-2018); PoMigra: Politically motivated crime in the light of current migration flows – a transnational situation report and development of practical prevention measures (Internal Security Fund – Germany 2016 -2018); EvoCS: The evolving concept of security: a critical evaluation across four dimensions (FP7, 2014-2016); IRISS: Increasing Resilience in Surveillance Societies (FP7, 2011 -2015); Countering Violent Extremism among Youth to Prevent Terrorism (NATO SPS Programme Advanced Research Workshop 2013 - 2014); ANDROID: disaster resilience network (FP7, 2011-2014); Smart Ciber: System of Maps Assessing Risk of Terrorism against Critical Infrastructures in Big Events Rallies (CIPS 2010 Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks, 2011-2013); ACRIMAS: Aftermath Crisis Management System-of-systems Demonstration (FP7 2011-2012); L4S: Learning 4 Security (FP7 2009 - 2011).

### [Contacts:](#)

**Prof. Marco Lombardi**

Director of the Department of Sociology

[marco.lombardi@unicatt.it](mailto:marco.lombardi@unicatt.it)



**FAR  
FACES**

## Anexo 5



# BITCENTER UK LTD

## FACE THE FUTURE

### FAST AND RELIABLE REAL-TIME MOBILE FACIAL RECOGNITION

[WWW.FARFACES.NET](http://WWW.FARFACES.NET)

Looking to join a consortium in

**HORIZON EUROPE**

**Call Reference:** HORIZON-CL3-2021-  
BM-01-02

**Title of call:** Increased safety,  
Security, performance of the European  
Border and Coast Guard and of  
European customs authorities.



# COMPANY AND SOLUTION

## THE COMPANY

### WHAT WE ARE

BitCenter UK Ltd (Breakthrough Information Technology Center) is a High-Tech Software Development company, founded in 2019 in London, UK., with the main area of interests - Computer Vision, Machine Learning and Convolutional DNNs.

The objective of the company is the creation and implementation of Objects and Facial Recognition software for mobile platforms. Our technology is B2B for civil defence or military forces (dual purpose solutions).

## SOLUTION

### WHAT WE DO

During the past two years our company BITCENTER UK LTD has developed a unique Facial Recognition Technology for mobile devices called **FarFaces**. The uniqueness of our technology is the distance between the mobile device and recognizing person. **We are still the ONLY company who managed to reach from 10 to 15 meters in Real-Time facial recognition**, using just a user's mobile phone or tablet, without any installations, specialists and additional costs.

## TEAM

### WHO WE ARE

Our core team of researchers, mathematicians, developers and engineers have over 15 years of experience in Computer Vision, Machine Learning and Deep Neural Networks.

## PARTNERS

### WHO WE WORK WITH

BitCenter collaborated on several projects with Lanit-Terkom (Italy), Sedicii (UK), Sitek (Italy)

# CONTRIBUTION TO A CONSORTIUM

**FarFaces** technology could offer a Consortium additional highly intelligent tool for public and personnel safety, efficiency, faster and better decision making.

01

## Expertise that can enhance a consortium

We would be happy to offer our technology and expertise to a consortium that could benefit from recent advancements in real-time facial and object recognition and its effectiveness at long distances, its accessibility on mobile devices creating new opportunities to leverage the technology for increased public safety. It could help law enforcement deter terrorism, prevent violent crime, identify wanted individuals and suspected terrorists, find missing persons as well as assist in mental health situations and post-event investigations. In addition to crime prevention benefits, facial recognition technology may increase officer safety by identifying people at a long distance (criminals, people with medical conditions, locating missing or abducted persons).

02

## Why we are the best organisation to have in the consortium

We are the only company in the market that offers a ready-made independent mobile solution for facial recognition. Our technology could also be customized and integrated with other existing technologies, such as CCTV systems, number plate recognition systems, drones, smart glasses and body-worn cameras.





# Mobile App Main Functions

RECOGNIZE ONLY PEOPLE WHO ARE IN THE DATABASE



RECOGNIZE ONLY PEOPLE WHO ARE NOT IN THE DATABASE



DETECT MORE THAN 20 PEOPLE IN LESS THAN A SECOND AND RECOGNIZE EVERYONE IN THE BACKGROUND



POSSIBILITY TO WORK OFFLINE WITH A DATABASE OF MORE THAN 12 MILLION FACES

Detect more than 20 faces per frame in less than one **second**

WE SAVE TIME AND MONEY FOR POLICE, SECURITY

PROBLEMS

SOLUTIONS

Save unlimited number of faces on the cloud and up to **12 million** faces locally



HISTORY LOG WITH GPS LOCATION

ADDING A PERSON TO THE DATABASE FROM MOBILE DEVICE



ASSIGN A DANGER LEVEL TO A RECOGNIZED PERSON BY COLORING THE FRAME AROUND FACE GREEN, YELLOW OR RED

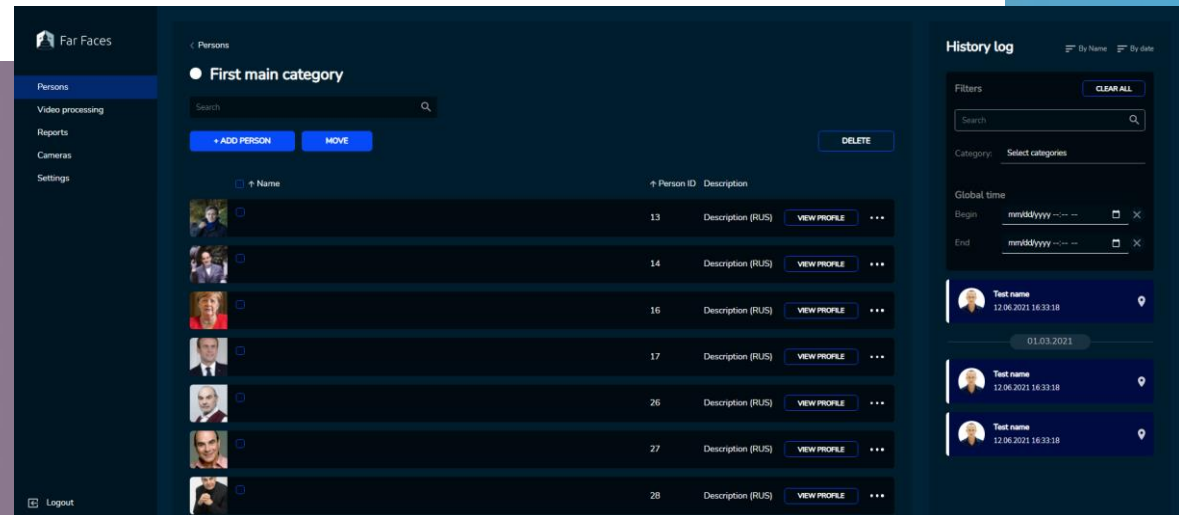
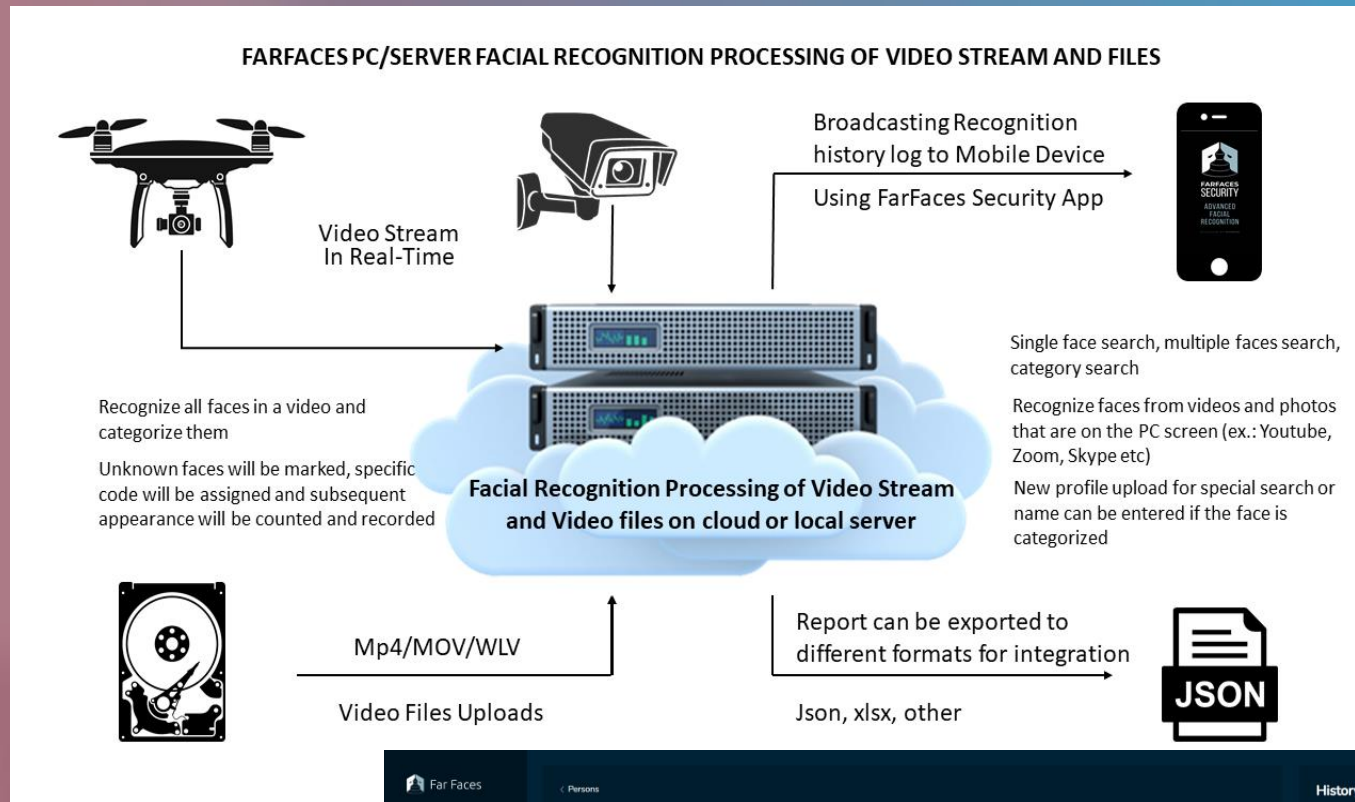


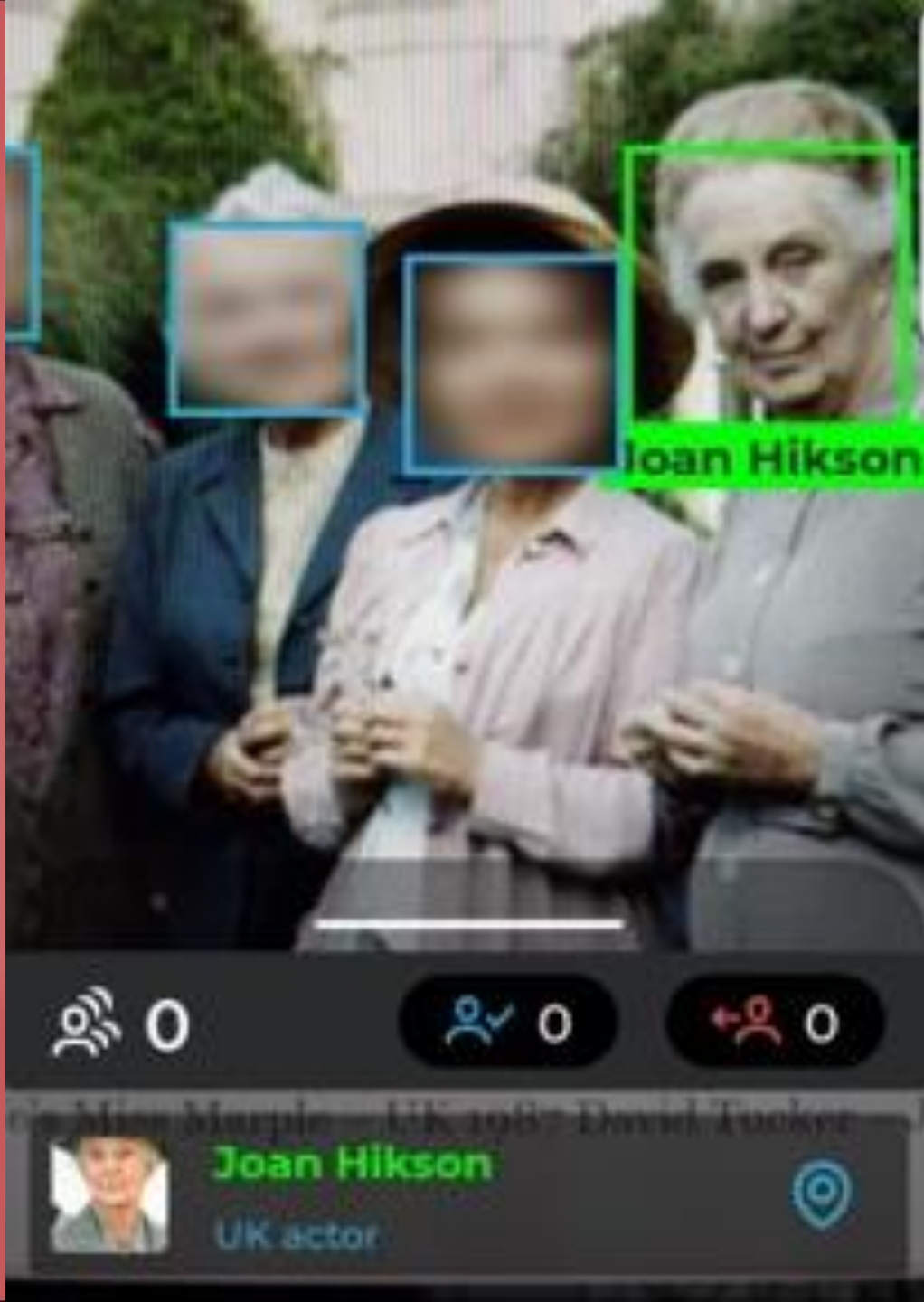
ABILITY TO SWITCH BETWEEN DIFFERENT DATABASES BY USING DIFFERENT ACCESS KEYS

# PC/SERVER Recognition

PC/Server Facial Recognition Software also developed by our company for real-time and post-processing of a video stream from any IP cameras, including cameras installed on UAVs, as well as from a screen ex. Zoom video conference, Skype, YouTube.

Our software's functions include the recognition of faces from any video stream as well as the ability to categorize and count the faces logged. Unknown faces can be identified and marked, with a specific code being assigned to them and allowing for their subsequent appearance to be counted and recorded for security purposes. The software also provides a history log with the date, time and number of each face recognized during any chosen period. Single face, multiple faces, and category searches are also available.





## “ To comply with GDPR

People who don't give consent will not be recognised, faces are blurred right away on a mobile device and no images are store anywhere. Meaning, if the person is not in a database of criminals he/she will not be recognised hence the algorithm blurred the faces.

Images of faces detected and recognised (in the RAM of the mobile device) are completely deleted from the system, even before the face descriptor (numerical vector containing a generalized image description and does not allow to restore the original face image in any way) and the personal data are compared. This means that the image of a face (or any image at all) is not transmitted over a network and is not stored in the system in any way, therefore the biometrics data will not be lost or stolen during the transition.

”

N A D Y A K R A M S K A Y A

Co-Founder and CEO



**BitCenter UK Ltd**  
Chief Executive Offices  
London, UK



## NADYA KRAMSKAYA

Experienced Director with a demonstrated track record of working in the Information Technology and Services industries. Skilled in Trading, Risk Management, Corporate Finance, Strategic Planning, and Business Development.



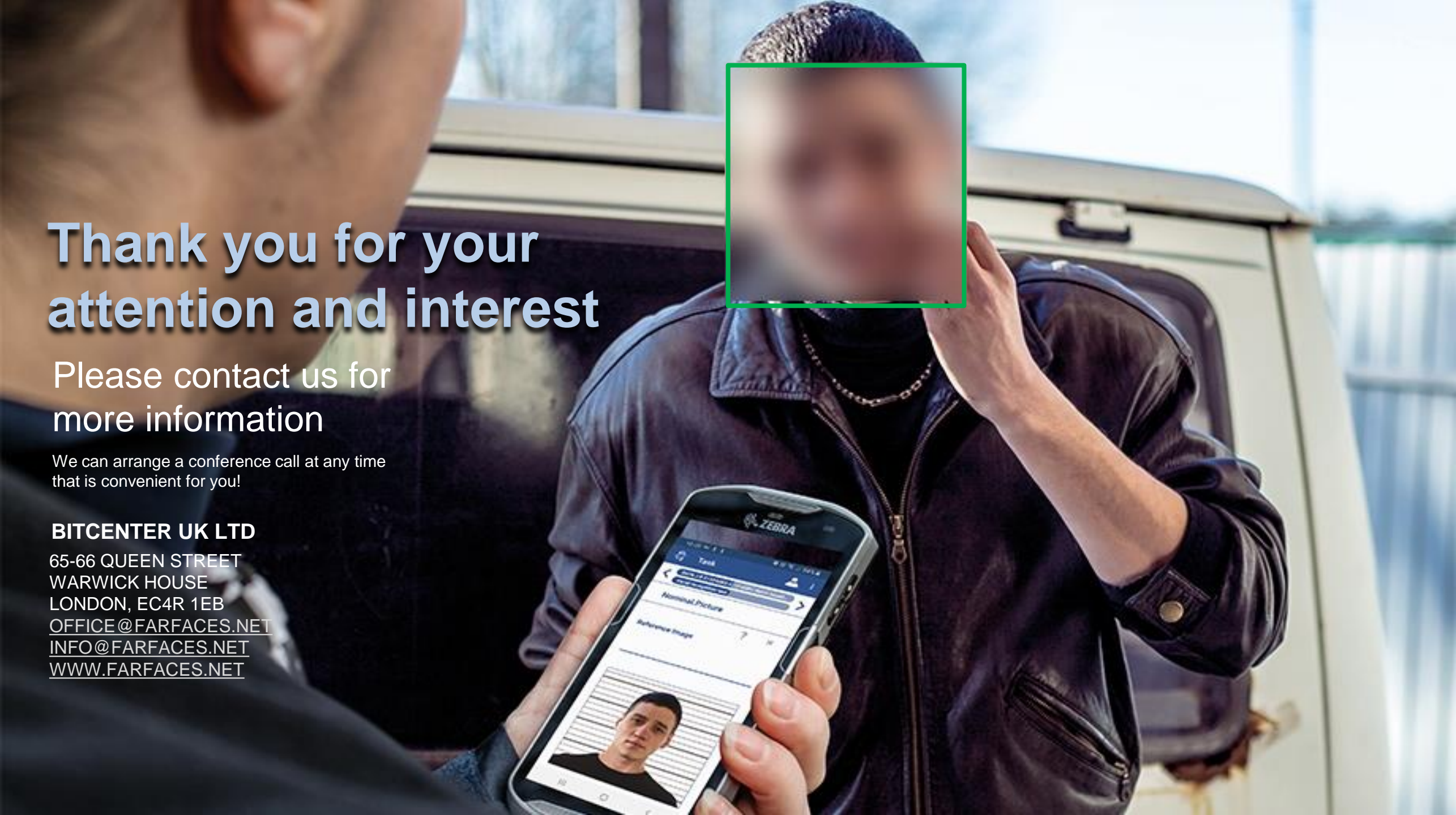
nk@bitcenter.eu

## ZALE JOHNSON

National Contact Point & Global Innovation Lead - Security



Zale.Johnson@innovateuk.ukri.org



# Thank you for your attention and interest

Please contact us for  
more information

We can arrange a conference call at any time  
that is convenient for you!

## **BITCENTER UK LTD**

65-66 QUEEN STREET  
WARWICK HOUSE  
LONDON, EC4R 1EB  
[OFFICE@FARFACES.NET](mailto:OFFICE@FARFACES.NET)  
[INFO@FARFACES.NET](mailto:INFO@FARFACES.NET)  
[WWW.FARFACES.NET](http://WWW.FARFACES.NET)

# Samurai Digital Security



**SAMURAI**  
DIGITAL SECURITY

Looking to join a consortium in  
HORIZON EUROPE

Call Reference: HORIZON-CL3-2021-CS-01-03

Title of Call: AI for cybersecurity reinforcement

# Who We Are and What We Do



- Samurai Security was established in 2016 by two leading cybersecurity academics. Success has seen the company grow and today the company employs 15 staff - many of whom are post-graduate trained cybersecurity experts- and been certified by the National Cyber Security Centre (NCSC)
- The company offers a broad spectrum of cybersecurity services including:
  - Security Assessments and Penetration Testing
  - Incident Response & Management
  - Regulatory Compliance
  - Cybersecurity / Data Protection Training (including GDPR and CREST)
- Samurai Security has worked with:
  - The Malta Information Technology Agency – collaborating to securely deliver a high-profile cryptocurrency conference.
  - The NHS - investigating the security of key systems following the 'Wannacry' security breach.
  - The International Organization for Migration - providing assurance and ensuring the security of the critical applications that protect their staff overseas are secure.

# Our Contribution to a Consortium



## Expertise Samurai can bring to a consortium:

- We have performed network intrusion detection for some of the largest financial, health and retail companies in the UK.
- Co-authored an award-winning and innovative research paper into the use of Artificial Intelligence (AI) and Machine Learning (ML) to detect malicious shell code.<sup>1</sup>
- A combined 20 years of academic and research experience spanning four universities.
- We would like to bring this existing expertise and research into a consortium to help reinforce cyber security posture without compromising on legal and ethical requirements.

1. Intelligent intrusion detection systems using artificial neural networks: <https://shura.shu.ac.uk/20882/10/Shenfield-IntelligentIntrusionDetection%28VoR%29.pdf>



# Our Technology Vision



- Many organisations are migrating to the cloud and aiming to become "zero trust" entities, but with disparate systems, cloud providers, web 2.0, etc it becomes hard to monitor and manage the security of these systems.
- Our proposed solution runs within a cloud environment, and monitors network traffic, (HTTP, SMB, etc) for malicious code.
- In order to combat typical issues with IDS/IPS systems, a detection engine based on machine learning and AI techniques as well as typical signature-based detections is to be employed.
- Our proposed system, with modern detection mechanisms, the ability to configure orchestration and response automation, will enable organisations moving to "zero trust" to be able to monitor and protect themselves in a world where there is no central network.

# Contact Details



- Dr David Day BSc., PhD.
  - Managing Director
  - [dday@samuraisecurity.co.uk](mailto:dday@samuraisecurity.co.uk)
- Neil Richardson BSc., MSc.
  - Technical Director
  - [nrichardson@samuraisecurity.co.uk](mailto:nrichardson@samuraisecurity.co.uk)
- Bob Drake BSc., MSc., MBA
  - Non-executive Director
  - [bdrake@samuraisecurity.co.uk](mailto:bdrake@samuraisecurity.co.uk)
- Jamie Londra MComp
  - Research and Development Manager
  - [jlondra@samuraisecurity.co.uk](mailto:jlondra@samuraisecurity.co.uk)



# Safe Citizens: Horizon Europe

Safe Citizens is a United Kingdom based public safety technology organisation with partners and clients globally including Governmental and UN Agencies, NGO's, large, medium and small corporates and academic institutions.

Safe Citizens specialises in enhancing situational awareness and geo-relevant communications to the public without compromising user privacy using proprietary mobile technology. Our platform enables organisations to gain increased situational awareness in risky or dangerous situations, identify those members of the public most at risk and issue appropriate instructions to secure their safety. The technology is mature and being used on 170+ million devices through a Software Development Kit (SDK) format.

## Technology Highlights

- 100% Anonymous
- Device battery drain reduced by 97% compared to normal device location services usage
- Accurate live location to 10m
- Live operator remote scenario management
- Increased after event analysis capabilities
- No third party is required to 'enable' the technology

## 2021 Ideal Project Area's

- **DRS01 - Societal Resilience: Increased risk Awareness and preparedness of citizens**
  - HORIZON-CL3-2021-DRS-01-01: Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards
- **DRS02 - Improved Disaster Risk Management and Governance**
  - HORIZON-CL3-2021-DRS-01-02: Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building
- **DRS03 - Strengthened capacities of first and second responders**
  - HORIZON-CL3-2021-DRS-01-05: Improved international cooperation addressing first responder capability gaps
- **SSRI 02 - Increased Innovation uptake**
  - HORIZON-CL3-2021-SSRI-01-04: Demand-led innovation for situation awareness in civil protection

## Other Areas of Interest

Our business and expertise are geared towards public safety and our direct interest is keeping people safe. Due to the nature of our technology we have use cases in other areas and industries including healthcare, heavy industries, travel among others.

We'd welcome discussions around how our technology can potentially aide other submissions. We're also keen to explore potential collaboration with partners with a view on 2022 requirements.

## Contact Details

To follow up please contact either:

Martin Hogan on either [martin.hogan@safe-citizens.com](mailto:martin.hogan@safe-citizens.com) or 07545 493 068.

Daniel de Wolf on either [daniel.dewolf@safe-citizens.com](mailto:daniel.dewolf@safe-citizens.com) or 07725 144 242.

# SSH input into CLUSTER 3 - FCT

## Proposed Approach

The success of operational capabilities for *fighting crime and terrorism* as defined in the WP relies on practitioners to use technology, data and procedures in an effective, reliable and unbiased way. Prevention, detection, intelligence and investigation capabilities need to be informed by evidence of how practitioners select, process, use and share information, in order to gain situational awareness, identify patterns and trends, and forecast vulnerabilities and threats.

**Professor Mandeep K. Dhmi** can fulfil the *SSH scope* of projects by offering state-of-the-art expertise on human judgment and decision-making, risk perception, and uncertainty communication, and cutting edge methodologies for validating the use of technology, data and procedures, as well as designing effective skills & training for law enforcement and security in a range of domains (e.g., trafficking goods, online identity theft, terrorism, sexual violence and exploitation, and disinformation).

## Relevant Experience and Track Record

Prof. Dhmi is an *internationally respected scientist* with expertise in Cognitive , Forensic and Decision Science, as well as Criminology. She is author of over 120 publications and is Editor of *Judgment and Decision Making*. She has a successful funding record and regularly reviews bids.

Prof. Dhmi has worked for DSTL (UK Ministry of Defence). She was UK representative on the NATO panel 'Assessment and Communication of Risk and Uncertainty to Support Decision Making'; subject matter expert on the US Intelligence Advanced Research Projects Activity SIRIUS Program; and advisor to GCHQ , Sentencing Council of England and Wales, and UK Metropolitan Police.

Prof. Dhmi's research has received many international awards including the 2020 SAS Panel Excellence Award from the NATO Science & Technology Organization.

## ANEXO 8



## Organisational Capabilities

Organisation is a London-based UK University with experience of hosting EU-funded research.

It's research facilities and capabilities include:

- Dedicated laboratories and specialist software for research with human participants.
- Research ethics approval committees.
- Up-to-date research library.
- Experts including in Science & Technology, Business and Law.
- Press office for dissemination.
- Research & Knowledge Exchange support.

## Administrative Information & Contact Details

Planning on being a Partner.

### Mandeep K Dhmi, PhD

#### Professor in Decision Psychology

Department of Psychology

Faculty of Science and Technology

Middlesex University

The Burroughs, Hendon, London, UK, NW4 4BT

**E-mail: [m.dhmi@mdx.ac.uk](mailto:m.dhmi@mdx.ac.uk)**

Organisation's PIC: 999883470